CA Enterprise Log Manager

Manuel de présentation

r12.1

La présente documentation ainsi que tout programme d'aide informatique y afférant (ci-après nommés "Documentation") vous sont exclusivement fournis à titre d'information et peuvent être à tout moment modifiés ou retirés par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

SOUS RESERVE DES DISPOSITIONS PREVUES PAR LA LOI APPLICABLE, CA FOURNIT LA PRESENTE DOCUMENTATION "TELLE QUELLE" SANS AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, NOTAMMENT AUCUNE GARANTIE DE LA QUALITE MARCHANDE, D'UNE QUELCONQUE ADEQUATION A UN USAGE PARTICULIER OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ETRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RESULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITE, PERTE DE DONNEES OU DE CLIENTS, ET CE MEME DANS L'HYPOTHESE OU CA AURAIT ETE EXPRESSEMENT INFORME DE LA POSSIBILITE DE LA SURVENANCE DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

La présente Documentation étant éditée par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2009 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA référencés

Ce document fait référence aux produits CA suivants :

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Security Compliance Manager (CA SCM)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Modifications de la documentation

Les actualisations suivantes ont été réalisées depuis la dernière version de la présente documentation.

- Présentation du démarrage rapide : cette rubrique existante a été mise à jour pour référencer des types d'événement, en plus des syslogs, pouvant être collectés par l'agent par défaut sur le serveur CA Enterprise Log Manager.
- Alerte de violation de stratégie : cette rubrique existante a été mise à jour de manière à référencer la possibilité d'envoyer des alertes sous forme d'interruptions SNMP à des systèmes de surveillance de la sécurité système et des alertes directes, pour exécuter un processus de sortie de l'événement/de l'alerte IT PAM, tel qu'un processus de création de tickets d'assistance.
- Explorer la bibliothèque de documentation : cette rubrique existante a été mise à jour pour référencer le nouveau Manuel de programmation de l'API, qui apparaît dorénavant sur la bibliothèque CA Enterprise Log Manager.

Informations complémentaires :

Présentation d'un déploiement rapide (page 15)
Alerte de violation de stratégie (page 56)
Exploration de la bibliothèque de documentation (page 65)

Table des matières

Chapitre 1 : Introduction 9

A propos de ce manuel 9
A propos de CA Enterprise Log Manager 10
Votre réseau avant l'installation 11
Eléments installés 12

Chapitre 2 : Déploiement rapide 15

Présentation d'un déploiement rapide 15
Installation d'un système à un seul serveur 16
Mise à jour de votre fichier hosts Windows 22
Configuration du premier administrateur 22
Configuration des sources d'événement Syslog 25
Modification du connecteur Syslog 29
Affichage d'événements Syslog 32

Chapitre 3 : Déploiement de l'agent Windows 35

Création d'un compte d'utilisateur pour l'agent 35
Définition de la clé d'authentification d'un agent 36
Téléchargement du programme d'installation de l'agent 37
Installation d'un agent 38
Création d'un connecteur basé sur NTEventLog 41
Configuration d'une source d'événement Windows 44
Affichage de journaux à partir de sources d'événement Windows 45

Chapitre 4 : Principales fonctionnalités 49

Collecte de journaux 49
Stockage des journaux 51
Présentation normalisée des journaux 53
Génération de rapports de conformité 54
Alerte de violation de stratégie 56
Gestion des droits 57
Accès selon un rôle 58
Gestion de l'abonnement 59
Contenu prêt à l'emploi 60

Chapitre 5 : Informations complémentaires concernant CA Enterprise Log Manager 61

Affichage des infobulles 61
Affichage de l'aide en ligne 63
Exploration de la bibliothèque de documentation 65

Glossaire 67

Index 97

Chapitre 1 : Introduction

Ce chapitre traite des sujets suivants :

A propos de ce manuel (page 9)
A propos de CA Enterprise Log Manager (page 10)

A propos de ce manuel

Ce *Manuel de présentation* traite de CA Enterprise Log Manager. Il débute par de rapides didacticiels qui vous permettent d'acquérir une première expérience du produit. Le premier didacticiel vous guide pour installer CA Enterprise Log Manager sur un seul serveur, l'exécuter et afficher des Syslogs collectés à partir d'unités UNIX à proximité sur le réseau. Le deuxième didacticiel vous guide pour installer un agent sur un système d'exploitation Windows, configurer la collecte de journaux et afficher les journaux d'événements qui en résultent. Il décrit ensuite les principales fonctions et indique les ressources permettant d'en savoir plus. Ce manuel a été conçu pour tous les publics.

Vous trouverez ci-dessous un récapitulatif du contenu.

Section	Description
A propos de CA Enterprise Log Manager	Intégrer CA Enterprise Log Manager dans votre environnement réseau actuel.
Déploiement rapide	Installer un système sur un seul serveur, configurer les sources d'événement Syslog, mettre à jour le connecteur Syslog pour l'agent par défaut et afficher les événements ajustés.
Déploiement de l'agent Windows	Préparer l'installation de l'agent, installer un agent pour le système d'exploitation Windows, configurer un connecteur pour la collecte avec agent, mettre à jour la source d'événement et afficher les événements générés.
Principales fonctionnalités	Profiter des principales fonctions, dont la collecte de journaux, le stockage des journaux, la génération de rapports de conformité et les alertes.
Informations complémentaires concernant CA Enterprise Log Manager	Obtenir les informations nécessaires par le biais des infobulles, de l'aide en ligne et de la bibliothèque documentaire.

Remarque : Pour plus de détails sur la prise en charge des systèmes d'exploitation ou la configuration système requise, consultez les *Notes de parution*. Pour disposer de procédures pas à pas sur l'installation de CA Enterprise Log Manager et la configuration initiale, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'installation d'un agent, consultez le *Manuel d'installation des agents*. Pour plus de détails sur l'utilisation et la maintenance du produit, consultez le *Manuel d'administration*. Pour obtenir de l'aide quant à l'utilisation d'une page CA Enterprise Log Manager, consultez l'aide en ligne.

A propos de CA Enterprise Log Manager

CA Enterprise Log Manager est axé sur la conformité et l'assurance informatiques. Il vous permet de collecter, de normaliser, de cumuler et de générer des rapports concernant l'activité informatique, mais également de générer des alertes nécessitant une action en cas de violations de la conformité. Vous pouvez collecter des données provenant d'unités disparates, sécurisées et non sécurisées.

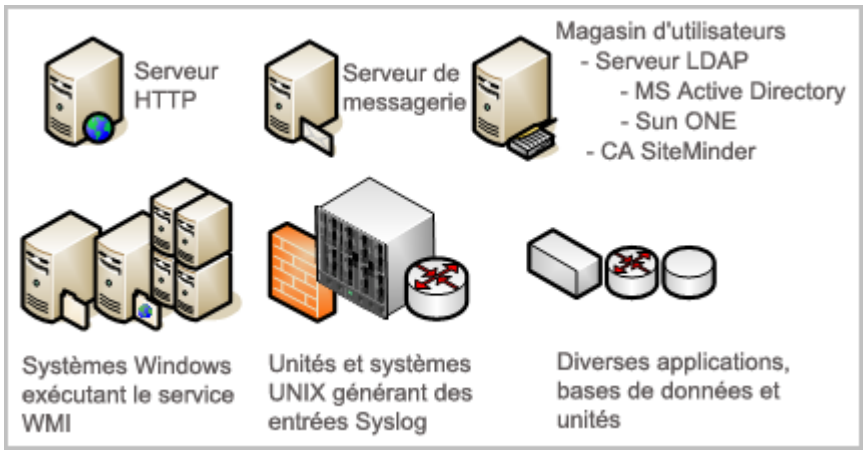
Votre réseau avant l'installation

Les réglementations et lois fédérales exigent la gestion des enregistrements de journaux. Par souci de conformité, vous devez.

- Autoriser l'accès aux journaux pour les audits.
- Stocker les journaux pendant plusieurs années.
- Restaurer les journaux à la demande.

Le grand nombre des enregistrements de journaux, leur emplacement et leur nature temporaire rendent difficile leur gestion. Les journaux sont continuellement générés par l'utilisateur et l'activité du processus sur le logiciel. Le taux de génération se mesure en événements par seconde (eps). Les événements bruts sont enregistrés sur chaque base de données, application et système actifs de votre réseau. La sauvegarde d'enregistrements de journaux doit se faire au niveau de chaque source d'événement avant qu'ils ne soient écrasés. La restauration des journaux d'événement est difficile quand des sources d'événement différentes sont stockées séparément.

Le format de la chaîne des événements bruts rend fastidieux leur interprétation car la sévérité de l'événement n'est pas évidente. Des données similaires peuvent également varier sur des systèmes différents.


Serveur HTTP
Serveur de messagerie
Magasin d'utilisateurs
- Serveur LDAP
- MS Active Directory
- Sun ONE
- CA SiteMinder
Systèmes Windows exécutant le service WMI
Unités et systèmes UNIX générant des entrées Syslog
Diverses applications, bases de données et unités

L'efficacité opérationnelle exige une solution qui regroupe tous les journaux, facilite leur lecture, automatise l'archivage et le stockage et rationalise leur restauration. CA Enterprise Log Manager offre ces avantages, et vous permet d'envoyer des alertes aux personnes et systèmes quand des événements critiques se produisent.

Eléments installés

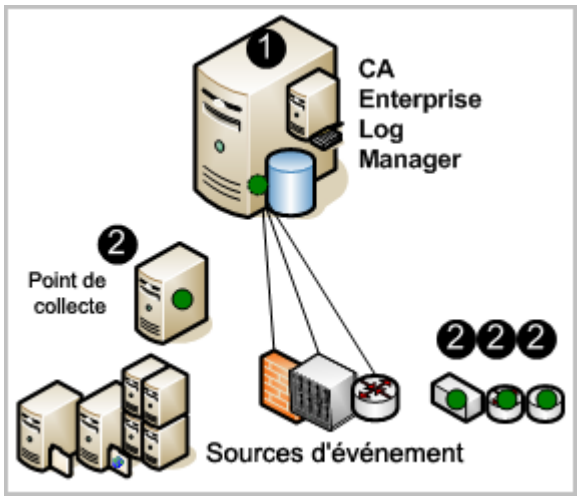
La configuration d'une solution avec un seul serveur et le lancement de la collecte d'événements prennent peu de temps.

Les disques d'installation incluent les composants ci-dessous.

- Système d'exploitation (Red Hat Enterprise Linux) pour le dispositif logiciel
- Serveur CA Enterprise Log Manager
- Agent CA Enterprise Log Manager (désigné ci-après par l'agent)

Dans l'illustration qui suit, CA Enterprise Log Manager est décrit comme un serveur comportant un petit serveur, un cercle sombre (vert) et une base de données. Le petit serveur représente le référentiel local de stockage de contenu au niveau des applications. Le cercle sombre représente l'agent par défaut et la base de données représente le magasin de journaux d'événements, où les journaux d'événements entrants sont traités et mis à disposition pour les requêtes et les rapports.

Les cercles sombres (verts) sur le point de collecte et les autres sources d'événement représentent des agents installés séparément. L'installation d'autres agents est facultative. Vous pouvez collecter des Syslogs provenant de sources d'événement compatibles avec UNIX grâce à l'agent par défaut, une fois la configuration requise terminée.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Vous installez le système d'exploitation pour le dispositif logiciel, puis vous installez l'application CA Enterprise Log Manager. Dès que vous configurez vos sources pour envoyer des Syslogs vers CA Enterprise Log Manager et que vous indiquez les cibles Syslog dans la configuration du connecteur pour l'agent par défaut, les Syslogs sont collectés et ajustés afin de simplifier leur interprétation.
2. (Facultatif) Vous pouvez installer un agent sur un hôte dédié comme point de collecte ou vous pouvez installer des agents directement sur les hôtes disposant des sources générant les événements que vous souhaitez collecter.

Remarque : Pour plus de détails sur l'installation du dispositif logiciel, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'installation des agents, consultez le *Manuel d'installation des agents*.

Informations complémentaires :

Installation d'un système à un seul serveur (page 16)
Installation d'un agent (page 38)

Chapitre 2 : Déploiement rapide

Ce chapitre traite des sujets suivants :

Présentation d'un déploiement rapide (page 15)
Installation d'un système à un seul serveur (page 16)
Mise à jour de votre fichier hosts Windows (page 22)
Configuration du premier administrateur (page 22)
Configuration des sources d'événement Syslog (page 25)
Modification du connecteur Syslog (page 29)
Affichage d'événements Syslog (page 32)

Présentation d'un déploiement rapide

Vous pouvez obtenir un déploiement CA Enterprise Log Manager simple et en état de fonctionnement avec un seul dispositif logiciel. Le connecteur Syslog prédéfini permet à l'agent par défaut de recevoir les événements générés par Syslog. Il vous suffit de configurer vos sources Syslog pour envoyer les événements Syslog vers CA Enterprise Log Manager et de modifier la configuration du connecteur Syslog pour identifier les cibles Syslog. Les données reçues dépendent de la bande passante entre le serveur et les sources Syslog, ainsi que de la latence.

Les capteurs de journaux, y compris WinRM et ODBC, prennent en charge les collectes directes de l'ensemble des journaux parmi plus de vingt sources d'événement autres que Syslog. Le capteur de journaux WinRM vous permet de collecter des événements directement à partir de serveurs exécutant Windows, comme le serveur Forefront Security pour Exchange, Forefront Security pour SharePoint Server, Microsoft Office Communication Server et le serveur virtuel Hyper-V, ainsi que des services, tels que les services de certificats Active Directory. Le capteur de journaux ODBC vous permet de capturer des événements générés par des bases de données Oracle9i ou SQL Server 2005. Pour plus de détails, consultez la matrice d'intégration de produits CA Enterprise Log Manager.

Pour installer CA Enterprise Log Manager, vous devez disposer des informations d'identification d'EiamAdmin. En tant que superutilisateur EiamAdmin, vous configurez un compte d'administrateur que vous utilisez pour effectuer la configuration. Si vous vous connectez en utilisant les informations d'identification de l'administrateur, vous pouvez vérifier que l'installation est correcte en visualisant des événements d'autosurveillance.

Installation d'un système à un seul serveur

Un système à un seul serveur constitue le déploiement le plus simple vous permettant d'effectuer des requêtes sur des événements et d'en afficher les résultats. Veillez à sélectionner un ordinateur respectant la configuration matérielle minimale pour un dispositif logiciel CA Enterprise Log Manager.

Remarque : Pour obtenir la liste du matériel certifié, les systèmes d'exploitation pris en charge et la configuration requise en termes de logiciel système et de services, consultez les *Notes de parution*.

Pour installer CA Enterprise Log Manager sur un système à un seul serveur

1. Conservez à votre disposition les informations ci-dessous.
   - Mot de passe de l'utilisateur root
   - Nom d'hôte pour votre dispositif
   - Si vous n'utilisez pas DHCP, l'adresse IP statique, le masque de sous-réseau et la passerelle par défaut de votre dispositif
   - Domaine du dispositif

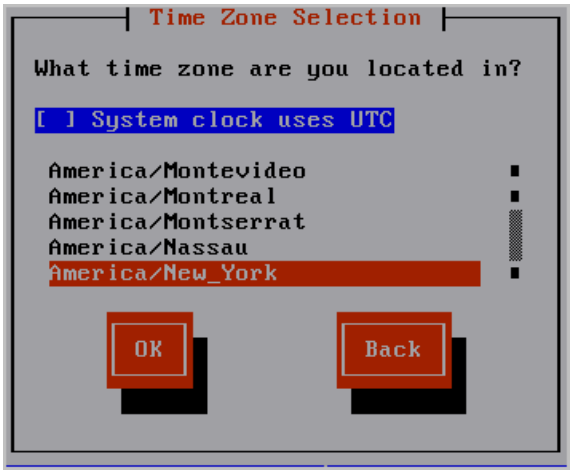
     Remarque : Le domaine doit être enregistré auprès des serveurs DNS de votre réseau pour que l'installation se termine correctement.
   - Adresse IP des serveurs DNS
   - Adresse IP de votre serveur de synchronisation NTP (facultatif)
   - Mot de passe du superutilisateur d'installation par défaut EiamAdmin
   - CAELM

     Il s'agit du nom d'application par défaut de l'application CA Enterprise Log Manager.

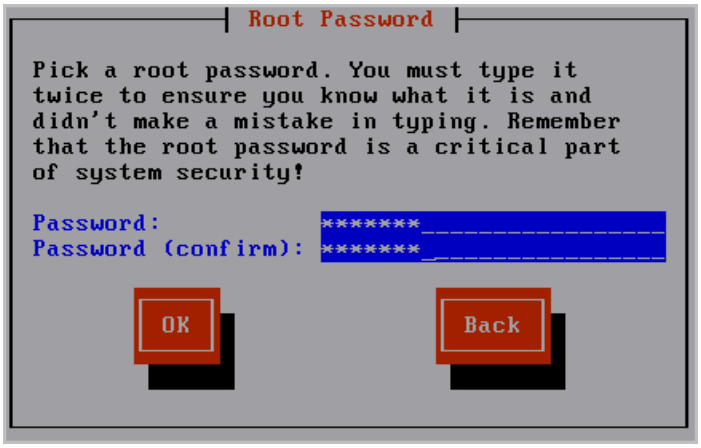
2. Installez le système d'exploitation préconfiguré à l'aide du média que vous avez créé à partir du package de téléchargement CA Enterprise Log Manager. Lors de l'installation du système d'exploitation, effectuez les opérations répertoriées ci-dessous.

   a. Choisissez un type de clavier. Par défaut, il s'agit d'un clavier Etats-Unis.

   b. Choisissez un fuseau horaire, par exemple America/New York, puis sélectionnez OK.



   c. Saisissez le mot de passe à utiliser comme mot de passe root, puis saisissez-le à nouveau pour le confirmer. Sélectionnez OK.


Root Password
Pick a root password. You must type it twice to ensure you know what it is and didn't make a mistake in typing. Remember that the root password is a critical part of system security!
Password:
Password (confirm):
OK
Back

Les informations relatives à la progression de l'installation apparaissent.

d. Retirez le disque d'installation du système d'exploitation, puis appuyez sur Entrée pour redémarrer le système.

Complete
Congratulations, your Red Hat Enterprise Linux Server installation is complete.
Remove any media used during the installation process and press <Enter> to reboot your system.
Reboot

Le système redémarre et entre en mode de démarrage non interactif. Il affiche les messages décrivant la progression de l'installation. Des informations détaillées sur cette installation sont enregistrées dans le fichier /tmp/pre-install_ca-elm.log.

L'invite ci-dessous s'affiche.

Please insert the CA Enterprise Log Manager r12 - Application Install disk and press enter.

3. Insérez le disque de l'application CA Enterprise Log Manager. Appuyez sur Entrée.

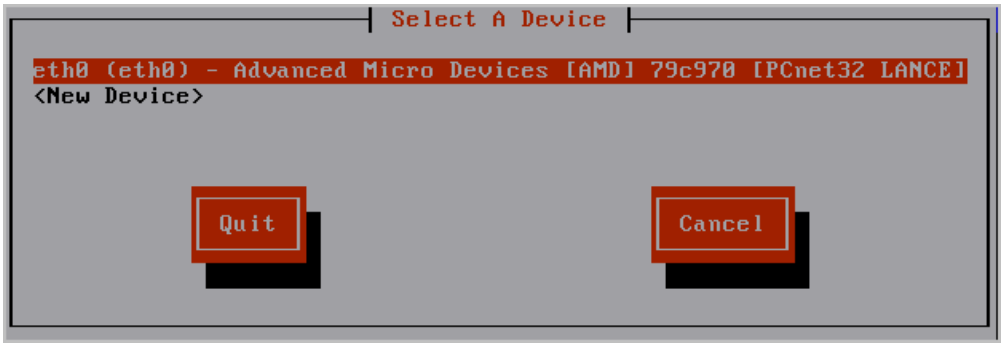
   Le processus d'installation vérifie si votre système respecte les spécifications minimales recommandées pour des performances optimales. Si tel n'est pas le cas, une invite s'affiche vous demandant si vous souhaitez arrêter ce processus d'installation.

   L'invite ci-dessous s'affiche.

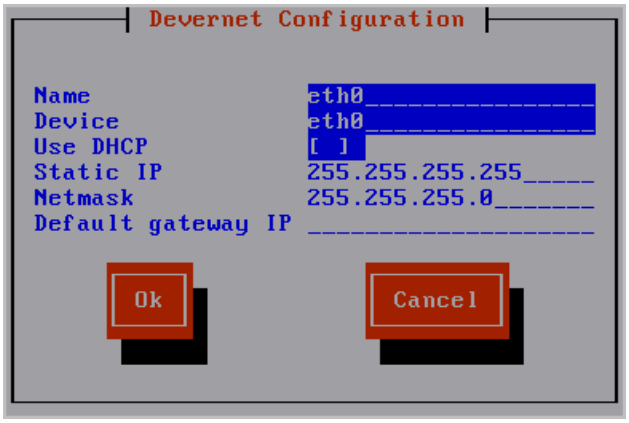
   Please enter a new hostname :

4. Entrez le nom d'hôte de ce dispositif logiciel CA Enterprise Log Manager. Par exemple, entrez CALM1.

5. Acceptez l'unité par défaut, eth0. Appuyez sur Entrée pour passer à l'écran suivant.



6. Effectuez l'une des opérations suivantes, puis sélectionnez OK.
   - Sélectionnez Use DHCP, une option acceptable uniquement pour un système de test autonome.
   - Entrez l'adresse IP statique, le masque de sous-réseau et l'adresse IP de la passerelle par défaut à associer au nom d'hôte que vous avez entré.



   Les services réseau sont redémarrés avec les nouveaux paramètres, qui sont affichés.

   Le message ci-dessous apparaît.

   Do you want to change the network configuration? (n) :

7. Vérifiez les paramètres du réseau. S'ils sont satisfaisants, saisissez "n" ou appuyez sur Entrée lorsqu'apparaît le message vous permettant de modifier les paramètres réseau.

   Le message ci-dessous apparaît.

   Please enter the domain name for this system :

8. Entrez votre nom de domaine, par exemple <votre_société>.com.

   Le message ci-dessous apparaît.

   Please enter a comma separated list of DNS servers to use:

9. Entrez les adresses IP de vos serveurs DNS internes, séparées par des virgules et sans espace.

   La date et l'heure de votre système s'affichent avec le message ci-dessous.

   Do you want to change the system date and time? (n)

10. Vérifiez la date et l'heure affichées du système. Si elles sont satisfaisantes, saisissez "n" ou appuyez sur Entrée.

    Le message ci-dessous apparaît.

    Do you want to configure the system to update the time through NTP?

11. Si vous souhaitez utiliser un serveur NTP (Network Time Protocol), continuez comme suit. Si tel n'est pas le cas, entrez "no" et passez à l'étape suivante.

    a. Répondez "yes" au message.

       Si vous spécifiez "yes", le message suivant apparaît.

       Please enter the NTP Server name or IP Address

    b. Entrez le nom d'hôte ou l'adresse IP du serveur NTP.

       Un message de confirmation similaire au message suivant apparaît :"Your system has been configured to update the time at midnight using the NTP server located at <yourntpserver>."

12. Lisez les contrats de licence d'utilisateur final présentés et répondez comme suit.

    a. Lisez le contrat de licence d'utilisateur final du kit de développement Sun Java (JDK).

       A la fin du contrat, le message ci-dessous apparaît.

       Do you agree to the above license terms? [yes or no]

    b. Saisissez "yes" si vous en acceptez les termes.

       Les informations d'enregistrement de produit sont affichées, suivies du message ci-dessous.

       Press Enter to continue.....

    c. Appuyez sur Entrée.

       Des messages indiquent qu'en préparation à l'installation CA Enterprise Log Manager, les paramètres système sont en cours de configuration. Le contrat de licence d'utilisateur final CA s'affiche.

    d. Lisez ce contrat de licence.

       A la fin du contrat, le message ci-dessous apparaît.

       Do you agree to the above license terms? [Yes or no]:

    e. Saisissez "Yes" si vous en acceptez les termes.

       Les informations de serveur CA EEM apparaissent.

13. Répondez aux invites suivantes pour configurer CA EEM.

    Do you use a local or remote EEM server?
    Enter l (local) or r (remote) :

    a. Pour créer un système de test autonome, entrez l pour local.

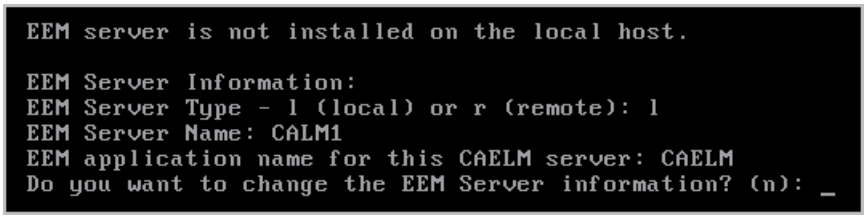
       Enter the password for the EEM server EiamAdmin user :
       Confirm the password for the EEM server EiamAdmin user :

b. Saisissez le mot de passe que vous souhaitez affecter au superutilisateur par défaut EiamAdmin ; saisissez-le à nouveau.

Enter an application name for this CAELM server (CAELM):

c. Appuyez sur Entrée pour accepter CAELM, le nom d'application par défaut de CA Enterprise Log Manager.

Les informations sur le serveur EEM que vous avez entrées jusqu'ici apparaissent avec un message vous demandant si vous souhaitez apporter des modifications.


EEM server is not installed on the local host.
EEM Server Information:
EEM Server Type - l (local) or r (remote): l
EEM Server Name: CALM1
EEM application name for this CAELM server: CAELM
Do you want to change the EEM Server information? (n): _

d. Appuyez sur Entrée ou saisissez "n" pour accepter les informations de serveur CA EEM que vous avez entrées.

Le processus d'installation démarre. Des messages indiquent la progression, à mesure de l'installation réussie de chaque composant CA Enterprise Log Manager, des enregistrements effectués, des certificats acquis, des fichiers importés et des composants configurés. Le message d'installation réussie de CA ELM apparaît. Lorsque l'installation se termine, le système affiche l'adresse de connexion de la console.

14. Notez cette adresse. Il s'agit de l'adresse que vous entrez dans un navigateur pour accéder à ce serveur CA Enterprise Log Manager, soit https://<nom_hôte>:5250/spin/calm.

    Une invite de connexion à <nom_hôte> apparaît. Vous pouvez l'ignorer.

    Remarque : Si, pour quelque raison que ce soit, vous souhaitez afficher l'invite du système d'exploitation à partir de cette invite de connexion, vous pouvez entrer caelmadmin et le mot de passe par défaut, qui est le mot de passe que vous avez affecté au compte de l'utilisateur EiamAdmin. Vous pouvez utiliser le compte caelmadmin pour vous connecter au dispositif, sur la console ou via SSH.

15. Continuez comme suit.

    - Si vous avez configuré une adresse IP statique, veillez à enregistrer cette adresse IP auprès des serveurs DNS spécifiés à l'étape 9.
    - Si vous avez configuré DHCP, mettez à jour votre fichier hosts sur l'ordinateur à partir duquel vous souhaitez naviguer pour atteindre ce serveur.
    - Accédez à l'adresse URL notée à l'étape 14, puis configurez le premier administrateur.

Mise à jour de votre fichier hosts Windows

Lors de l'installation CA Enterprise Log Manager, vous pouvez identifier un ou plusieurs serveurs DNS ou sélectionner l'utilisation de DHCP. Si vous avez sélectionné DHCP, vous devez mettre à jour le fichier hosts Windows, à l'aide de votre navigateur, sur l'ordinateur à partir duquel vous souhaitez accéder à CA Enterprise Log Manager.

Pour mettre à jour votre fichier hosts sur l'hôte avec votre navigateur

1. Ouvrez l'explorateur Windows et accédez à C:\WINDOWS\system32\drivers\etc.
2. Ouvrez le fichier hosts au moyen d'un éditeur, par exemple Bloc-notes.
3. Ajoutez une entrée contenant l'adresse IP du serveur CA Enterprise Log Manager et le nom d'hôte correspondant.
4. Dans le menu Fichier, sélectionnez Enregistrer, puis fermez le fichier.

Configuration du premier administrateur

Après avoir installé CA Enterprise Log Manager avec un seul serveur, pour préparer sa configuration, accédez à l'URL du CA Enterprise Log Manager à partir d'une station de travail distante, connectez-vous et créez un compte d'administrateur que vous pouvez utiliser pour effectuer la configuration.

Remarque : Dans le cadre de ce déploiement rapide, nous acceptons le magasin d'utilisateurs par défaut et les stratégies de mots de passe par défaut. En général, ces éléments sont configurés avant l'ajout du premier administrateur.

Pour configurer le premier administrateur

1. A partir de votre navigateur, connectez-vous à l'URL ci-dessous, où nom_hôte est le nom d'hôte ou l'adresse IP du serveur sur lequel vous avez installé CA Enterprise Log Manager.

   https://<nom_hôte>:5250/spin/calm

2. Si une alerte de sécurité survient, procédez comme suit.

   a. Cliquez sur Afficher le certificat.

   b. Cliquez sur Installer le certificat, acceptez les valeurs par défaut, puis terminez l'assistant d'importation.

      Un avertissement de sécurité s'affiche et indique que vous êtes sur le point d'installer un certificat qui déclare représenter le nom d'hôte du serveur CA Enterprise Log Manager.

   c. Cliquez sur Oui.

      Le certificat racine est installé et un message s'affiche indiquant que l'importation s'est correctement terminée.

   d. Cliquez sur OK.

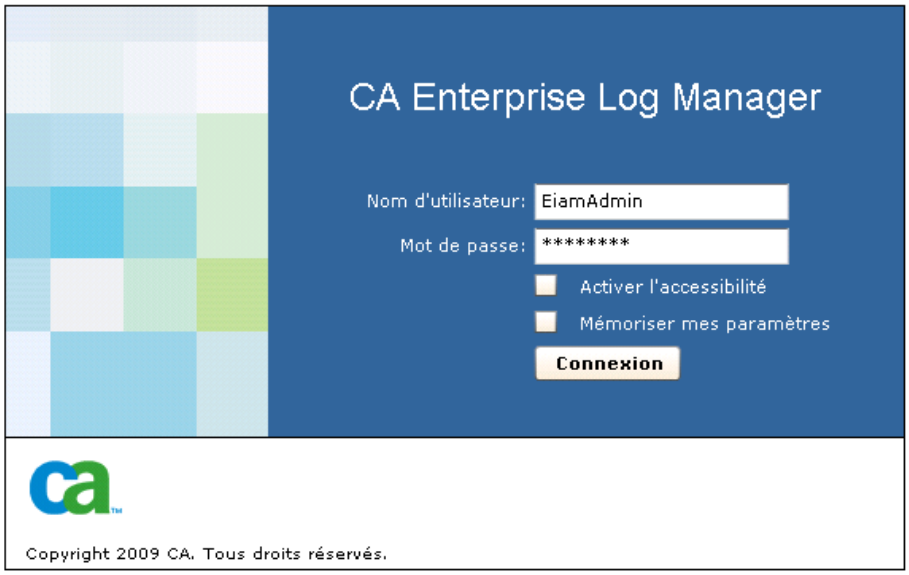
      La boîte de dialogue Certificat fiable s'affiche.

   e. Cliquez sur le chemin de certification et vérifiez que l'état du certificat indique que ce dernier est fiable (facultatif).

   f. Cliquez sur OK, puis sur Oui.

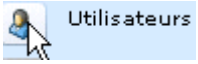
      La page de connexion apparaît.

3. Connectez-vous avec le nom d'utilisateur EiamAdmin et le mot de passe que vous avez créé lorsque vous avez installé le logiciel. Cliquez sur Connexion.

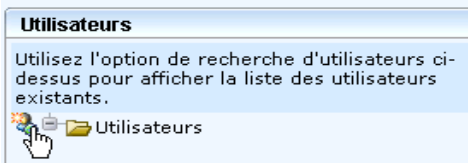


   L'application s'ouvre ; seuls l'onglet Administrator et le sous-onglet Gestion des utilisateurs et des accès sont actifs.

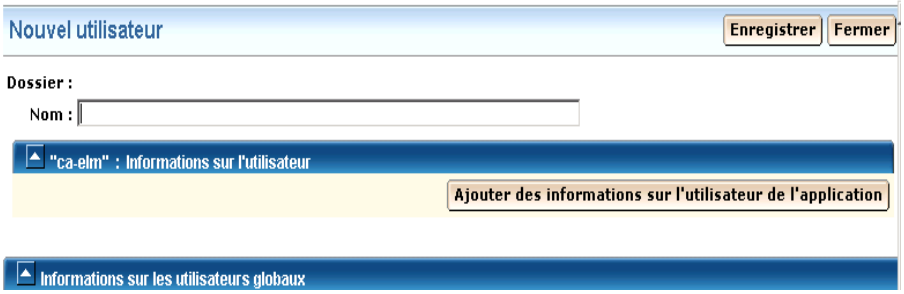
4. Cliquez sur Utilisateurs.



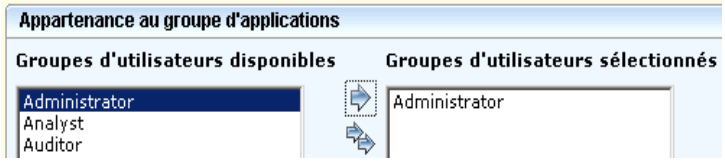
5. Cliquez sur Ajouter un nouvel utilisateur.


Utilisateurs
Utilisez l'option de recherche d'utilisateurs ci-dessus pour afficher la liste des utilisateurs existants.
Utilisateurs

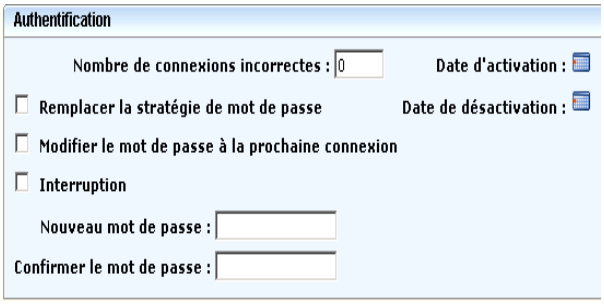
6. Entrez votre nom dans le champ Nom, puis cliquez sur Ajouter les détails de l'utilisateur de l'application.



7. Sélectionnez Administrator, puis placez-le dans la liste Groupes d'utilisateurs sélectionnés.



8. Sous Authentification, entrez un mot de passe pour ce nouveau compte dans le champ d'entrée, puis dans celui de confirmation.


Authentification
Nombre de connexions incorrectes : 0
Date d'activation :
Remplacer la stratégie de mot de passe
Date de désactivation :
Modifier le mot de passe à la prochaine connexion
Interruption
Nouveau mot de passe :
Confirmer le mot de passe :

9. Cliquez sur Enregistrer, puis sur Fermer. Cliquez sur Fermer.
10. Cliquez sur le lien Déconnexion de la barre d'outils.

    La page de connexion apparaît.

11. Connectez-vous à nouveau à CA Enterprise Log Manager avec les informations d'identification de l'administrateur que vous venez de définir.

    CA Enterprise Log Manager s'ouvre ; toutes les fonctionnalités sont activées. L'onglet Requêtes et rapports et le sous-onglet Requêtes sont affichés.

12. Affichez vos tentatives de connexion comme suit (facultatif).

    a. Dans la liste de balises de requête, sélectionnez Accès au système.

    b. Dans la liste de requêtes, sélectionnez Détail d'accès au système.

    Les résultats de la requête présentent vos deux tentatives de connexion, tout d'abord en tant qu'EiamAdmin, puis avec votre nom d'administrateur ; les tentatives de connexion sont marquées S pour successful (réussie).

Sévérité CA	Date	Compte	Exécutant	Hôte	Nom du jo...	Catégorie	Action	Résultat
Informations	Ven. 13 nov. 2009 5:33:26		-	SONMI02G2	NT-Security	System Access	Login Attempt	S
Informations	Ven. 13 nov. 2009 5:33:26	ANONYMOUS LOGON		SONMI02G2	NT-Security	System Access	Logoff	S
Informations	Ven. 13 nov. 2009 5:33:24	ANONYMOUS LOGON		SONMI02G2	NT-Security	System Access	Logoff	S
Informations	Ven. 13 nov. 2009 5:33:24		-	SONMI02G2	NT-Security	System Access	Login Attempt	S

Informations complémentaires :

Installation d'un système à un seul serveur (page 16)

Configuration des sources d'événement Syslog

Pour permettre à l'agent par défaut situé sur chaque serveur CA Enterprise Log Manager de collecter directement des événements Syslog, vous devez tout d'abord identifier les sources de ces événements, puis déterminer leur intégration associée. Vous pouvez ensuite effectuer les deux opérations suivantes dans l'ordre de votre choix.

- Configurez les sources d'événement Syslog. Connectez-vous à chaque hôte exécutant une source d'événement Syslog, puis configurez celle-ci conformément au manuel du connecteur de cette intégration Syslog.
- Configurez le connecteur Syslog sur l'agent par défaut afin d'ajouter les intégrations Syslog cibles associées aux sources d'événement configurées.

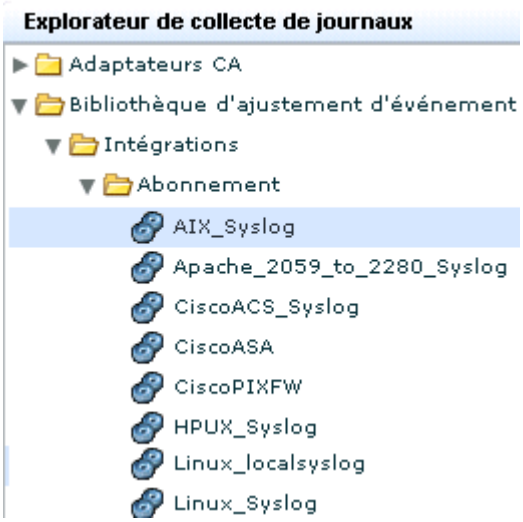
Dès que vous avez terminé ces deux étapes de configuration, la collecte et l'ajustement des événements commence. Vous pouvez ensuite utiliser CA Enterprise Log Manager pour afficher les événements qui vous intéressent ou générer des rapports à leur sujet, sous un format standardisé. Vous pouvez également générer des alertes lorsque des événements précis surviennent.

Pour configurer une source d'événement Syslog sélectionné

1. Connectez-vous à l'hôte sur lequel se trouve la source d'événement Syslog cible.
2. A partir d'un navigateur, lancez CA Enterprise Log Manager sur cet hôte.
3. Cliquez sur l'onglet Administration, puis sur le sous-onglet Collecte de journaux.

   L'explorateur de collecte de journaux s'affiche.
4. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement.

   La liste des intégrations prédéfinies s'affiche. Un exemple abrégé est présenté ci-dessous.



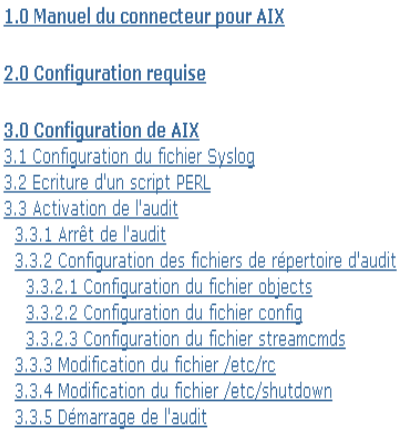
5. Sélectionnez l'intégration de la source d'événement que vous souhaitez configurer. Par exemple, si vous souhaitez collecter des Syslogs générés par un système d'exploitation AIX, vous devez sélectionner AIX_Syslog.

   Les détails de l'intégration apparaissent.

6. Cliquez sur le bouton Aide situé juste au-dessus du nom de l'intégration dans le volet droit.

   Le manuel du connecteur pour l'intégration sélectionnée apparaît.

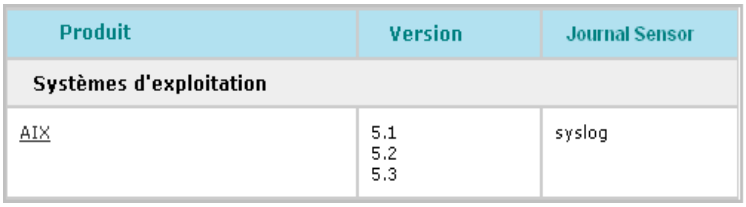
7. Cliquez sur la section relative à la configuration requise par la source d'événement. Dans cet exemple, la documentation décrit la configuration de la source d'événement du système d'exploitation AIX pour envoyer ses Syslogs à CA Enterprise Log Manager.


1.0 Manuel du connecteur pour AIX
2.0 Configuration requise
3.0 Configuration de AIX
3.1 Configuration du fichier Syslog
3.2 Ecriture d'un script PERL
3.3 Activation de l'audit
3.3.1 Arrêt de l'audit
3.3.2 Configuration des fichiers de répertoire d'audit
3.3.2.1 Configuration du fichier objects
3.3.2.2 Configuration du fichier config
3.3.2.3 Configuration du fichier streamcmds
3.3.3 Modification du fichier /etc/rc
3.3.4 Modification du fichier /etc/shutdown
3.3.5 Démarrage de l'audit

Exemple d'une autre source de manuels de connecteurs : le support en ligne

Vous pouvez ouvrir un manuel de connecteur sélectionné à partir de l'interface utilisateur CA Enterprise Log Manager ou du support en ligne de CA. L'exemple ci-dessous présente l'ouverture d'un manuel de connecteur à partir de cette autre possibilité.

1. Connectez-vous au support en ligne de CA.
2. Sélectionnez CA Enterprise Log Manager dans la liste déroulante de sélection d'une page de produit.
3. Faites défilez jusqu'à l'état du produit et sélectionnez la matrice de certification de CA Enterprise Log Manager.
4. Sélectionnez la matrice d'intégration du produit.
5. Recherchez la catégorie de l'intégration associée à la source d'événement que vous configurez. Par exemple, si la source d'événement est le système d'exploitation AIX, faites défiler jusqu'à la catégorie des systèmes d'exploitation, puis cliquez sur le lien AIX.



Produit	Version	Journal Sensor
Systèmes d'exploitation		
AIX	5.1 5.2 5.3	syslog

Modification du connecteur Syslog

Chaque CA Enterprise Log Manager comporte un agent par défaut. Lorsque CA Enterprise Log Manager est installé, son agent par défaut comporte un connecteur partiellement configuré appelé Syslog_Connector, basé sur l'écouteur Syslog. Cet écouteur reçoit des événements Syslog bruts sur les ports par défaut, dès que vous configurez les sources d'événement pour envoyer des Syslogs à CA Enterprise Log Manager. Toutefois, si vous souhaitez que CA Enterprise Log Manager ajuste ces événements bruts, vous devez modifier ce Syslog_Connector. Certaines modifications sont obligatoires et d'autres facultatives.

- Vous devez identifier les cibles Syslog lorsque vous modifiez ce connecteur. Vous sélectionnez en tant que cibles Syslog chaque intégration correspondant à une ou plusieurs sources d'événement configurées ou prévues. Votre identification de cibles Syslog permet à CA Enterprise Log Manager d'ajuster ces événements correctement.
- Si vous le souhaitez, vous pouvez appliquer des règles de suppression, limiter l'acceptation de Syslogs à des hôtes de confiance, spécifier les ports à écouter autres que 514 (port UDP Syslog réservé) et 1468 (port TCP par défaut), et/ou ajouter un nouveau fuseau horaire pour un hôte fiable.

Pour modifier le connecteur Syslog d'un agent par défaut

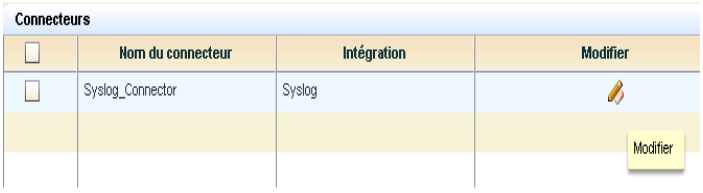
1. Cliquez sur l'onglet Administration.

   Le sous-onglet Collecte de journaux s'affiche.

2. Développez l'Explorateur d'agent, puis le groupe d'agents par défaut ou le groupe défini par l'utilisateur comportant CA Enterprise Log Manager à configurer.

3. Sélectionnez le nom d'un serveur CA Enterprise Log Manager.

   Le connecteur appelé Syslog_Connector s'affiche.



4. Cliquez sur Modifier.

   L'assistant de modification d'un connecteur apparaît ; l'étape Détails du connecteur est sélectionnée.

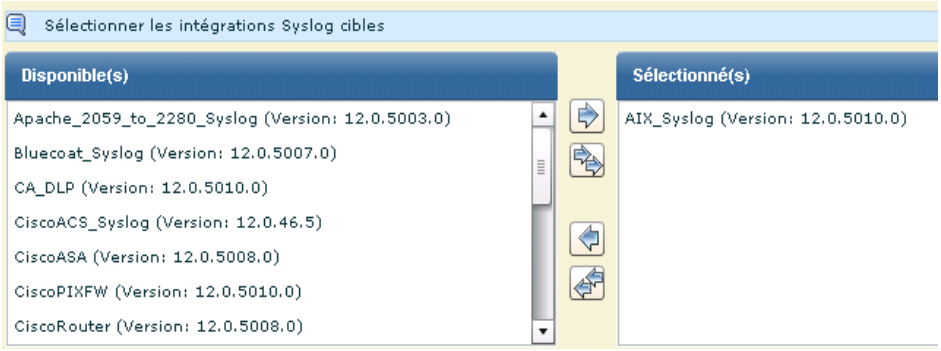
5. Cliquez sur Appliquer les règles de suppression (facultatif). Si vous souhaitez supprimer un type d'événement Syslog, c'est-à-dire si vous souhaitez qu'il ne soit *pas* collecté, faites-le passer de la liste Disponible(s) à la liste Sélectionné(s). Sélectionnez l'événement à déplacer, puis cliquez sur le bouton Déplacer.

6. Cliquez sur l'étape Configuration du connecteur.

   Toutes les intégrations disponibles sont sélectionnées par défaut.

7. Sélectionnez les cibles Syslog en faisant passer les intégrations Syslog à cibler de la liste Disponible(s) à la liste Sélectionné(s).

   Par exemple, si vous avez configuré le système d'exploitation AIX sur un hôte de votre réseau, vous faites passer la cible Syslog, AIX_Syslog, de la liste Disponible(s) à la liste Sélectionné(s).



8. Identifiez les hôtes fiables d'où proviennent les événements entrants acceptés par le connecteur Syslog (facultatif). Entrez l'adresse IP dans le champ d'entrée, puis cliquez sur Ajouter. Répétez cette procédure pour chaque hôte fiable. Tout événement reçu d'un hôte non configuré comme fiable est alors rejeté.

   Remarque : Il est recommandé de configurer des hôtes fiables. En général, vous configurez tous les hôtes sur lesquels vous avez établi des sources d'événement pour envoyer des Syslogs à CA Enterprise Log Manager. La spécification d'hôtes fiables assure que l'agent par défaut refuse les événements provenant de systèmes non autorisés qu'un attaquant a configurés pour envoyer des événements à l'écouteur Syslog.

9. Ajoutez des ports (facultatif).

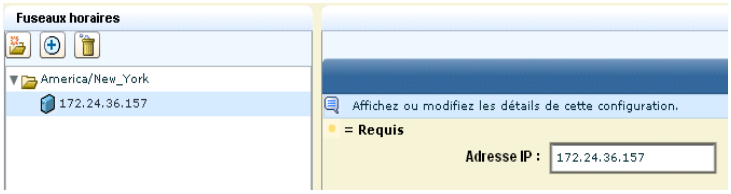
   En général, vous acceptez les ports UDP et TCP par défaut pour l'agent par défaut.

   Remarque : Vous pouvez améliorer les performances en définissant un connecteur Syslog pour différents types d'événements et en spécifiant un port différent pour chaque connecteur. Veillez à sélectionner des ports non utilisés lorsque vous affectez de nouveaux ports.

10. Ajoutez un fuseau horaire uniquement si vous collectez des Syslogs provenant d'ordinateurs situés dans un fuseau horaire différent de celui du dispositif logiciel (facultatif).

    a. Cliquez sur Créer un dossier, puis développez le dossier.

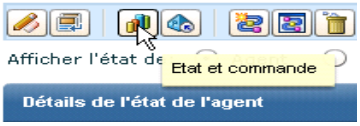
    b. Mettez en surbrillance l'entrée vide située sous le dossier. Entrez l'adresse IP d'un hôte fiable que vous avez configuré pour ce connecteur ou celle du serveur de synchronisation NTP que vous avez spécifié lors de l'installation de CA Enterprise Log Manager.



11. Cliquez sur Enregistrer et fermer.

12. Affichez l'état.

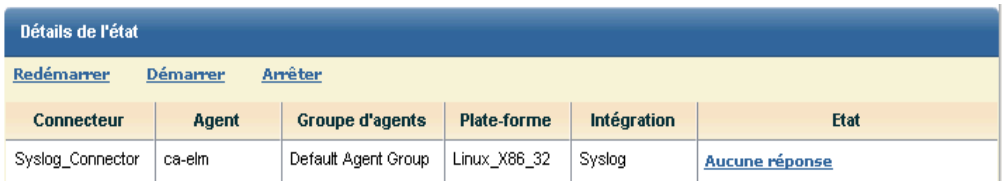
    a. Cliquez sur Etat et commande.



    Afficher l'état des agents est sélectionné. Comme l'agent par défaut se trouve sur ce serveur, le nom d'hôte du serveur que vous avez installé apparaît dans la colonne Agent. L'état affiché est Exécution en cours.

    b. Cliquez sur le lien Exécution en cours pour afficher les détails.

    c. Cliquez sur le bouton Connecteurs pour afficher l'état des connecteurs.



d. Cliquez sur le lien Exécution en cours.

Le pourcentage d'UC, l'utilisation de la mémoire, le nombre moyen d'événements par secondes et le nombre d'événements filtrés apparaissent.

Affichage d'événements Syslog

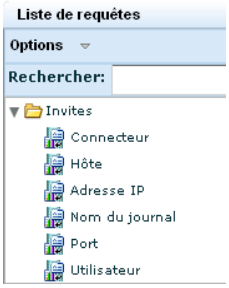
Pour afficher rapidement les résultats d'une requête sur des événements collectés par un écouteur Syslog, utilisez l'invite Hôte.

Pour afficher des événements Syslog

1. Sélectionnez l'onglet Requêtes et rapports.

   Le sous-onglet Requêtes s'affiche.

2. Développez Invites sous Liste de requêtes, puis sélectionnez Hôte.

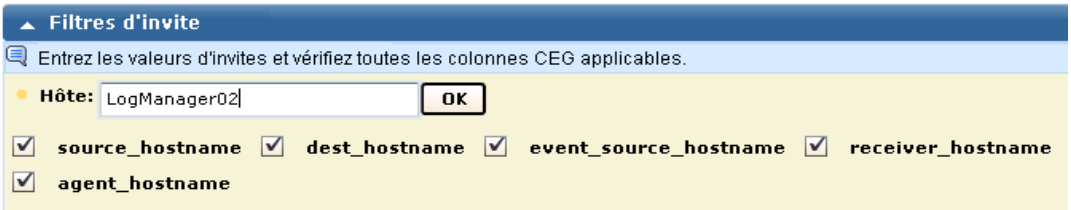


3. Soumettez une requête pour les événements collectés par l'agent par défaut.

   a. Dans le champ Hôte, entrez le nom d'hôte de l'agent par défaut ; il s'agit également du nom du CA Enterprise Log Manager sur lequel il réside.

   b. Sélectionnez agent_hostname.

   c. Cliquez sur OK.



4. Affichez les résultats à examiner.

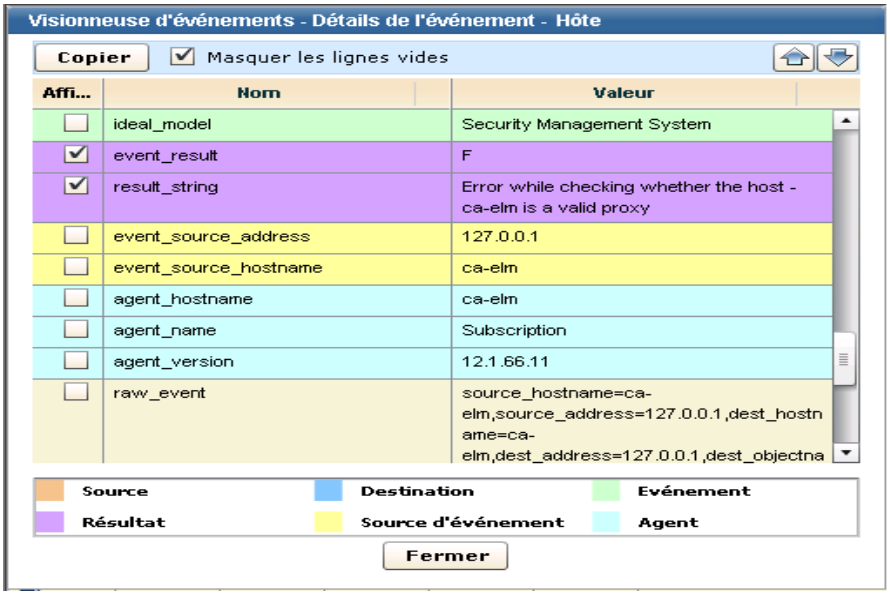
   a. Pour trier par résultats, cliquez sur la colonne Résultats.

   b. Faites défiler jusqu'au premier résultat F pour failure (échec). Supposez qu'il s'agit d'un avertissement de configuration de la catégorie Gestion de la configuration.

   c. Double-cliquez pour sélectionner la ligne à afficher en détail.

   La visionneuse d'événements apparaît.

5. Faites défiler jusqu'à la zone d'affichage du résultat. Dans cet exemple, l'erreur est un avertissement vous indiquant que vous devez configurer le module d'abonnement. Il s'agit d'un avertissement que vous devez ignorer jusqu'à la fin de l'installation de tous les serveurs CA Enterprise Log Manager souhaités.



Chapitre 3 : Déploiement de l'agent Windows

Ce chapitre traite des sujets suivants :

Création d'un compte d'utilisateur pour l'agent (page 35)
Définition de la clé d'authentification d'un agent (page 36)
Téléchargement du programme d'installation de l'agent (page 37)
Installation d'un agent (page 38)
Création d'un connecteur basé sur NTEventLog (page 41)
Configuration d'une source d'événement Windows (page 44)
Affichage de journaux à partir de sources d'événement Windows (page 45)

Création d'un compte d'utilisateur pour l'agent

Avant d'installer un agent sous Windows, vous devez créer un nouveau compte pour l'agent dans le dossier Utilisateurs de Windows. Ce compte avec peu de droits permet à l'agent de s'exécuter avec le moins de droits possibles. Lorsque vous installez l'agent, vous devez fournir le nom d'utilisateur et le mot de passe que vous avez créés ici.

Remarque : Vous pouvez omettre cette étape et spécifier les informations d'identification du domaine d'un administrateur pour l'agent lorsque vous installez ce dernier, mais cela n'est pas recommandé.

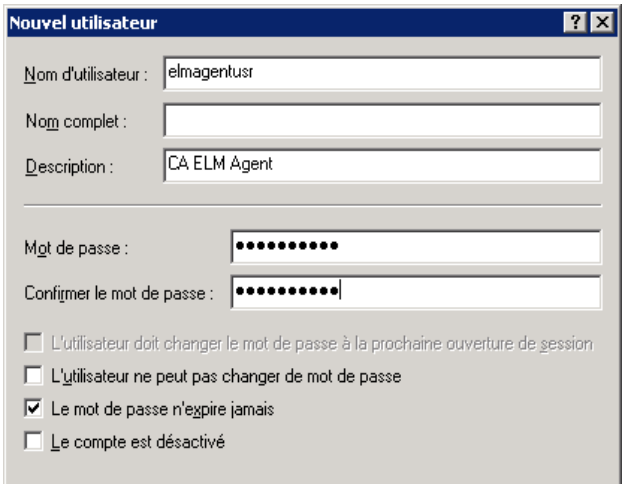
Pour créer un compte d'utilisateur Windows pour l'agent

1. Connectez-vous à l'hôte sur lequel vous souhaitez installer l'agent. Utilisez les informations d'identification de l'administrateur.
2. Cliquez sur Démarrer, Programmes, Outils d'administration, Gestion de l'ordinateur.
3. Développez Utilisateurs et groupes locaux.
4. Cliquez avec le bouton droit sur Utilisateurs et sélectionnez Nouvel utilisateur.

   La boîte de dialogue Windows Nouvel utilisateur apparaît.

5. Entrez un nom d'utilisateur, puis entrez deux fois un mot de passe. Un mot de passe sûr comporte une combinaison de caractères alphabétiques, numériques et spéciaux. Par exemple agent_calmr12. Saisissez une description (facultatif).

   Important : N'oubliez pas ce nom et ce mot de passe, ou notez-les. Vous en aurez besoin lorsque vous installerez l'agent.


Nouvel utilisateur
Nom d'utilisateur :
elmagentusr
Nom complet :
Description :
CA ELM Agent
Mot de passe :
Confirmer le mot de passe :
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Le compte est désactivé

6. Cliquez sur Créer. Cliquez sur Fermer.

Informations complémentaires :

Installation d'un agent (page 38)

Définition de la clé d'authentification d'un agent

Avant d'installer le premier agent, vous devez connaître la clé d'authentification de celui-ci. Vous pouvez utiliser la valeur par défaut, si aucune clé n'a été définie, utiliser la clé en cours, si elle est définie, ou définir une nouvelle clé. La clé d'authentification de l'agent configurée ici doit être entrée lors de l'installation de chaque agent. Seul un administrateur peut effectuer cette tâche.

Pour définir la clé d'authentification d'un agent

1. Ouvrez le navigateur sur l'hôte où vous souhaitez installer l'agent, puis entrez l'URL du serveur CA Enterprise Log Manager pour cet agent. Voici un exemple.

   https://<adresse_IP>:5250/spin/calm/

2. Connectez-vous à CA Enterprise Log Manager. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur Se connecter.
3. Cliquez sur l'onglet Administration.

L'explorateur de collecte de journaux s'affiche dans le volet gauche.

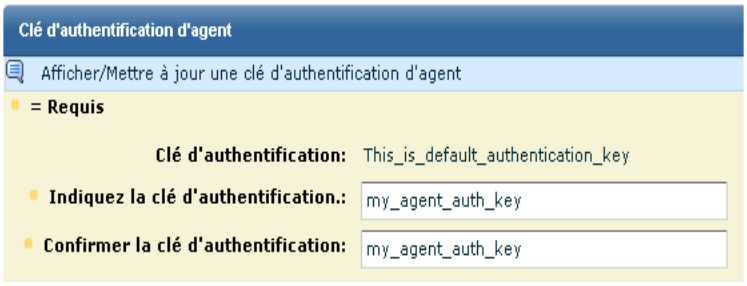
4. Sélectionnez le dossier de l'Explorateur d'agent.

   Une barre d'outil apparaît dans le volet principal.

5. Cliquez sur Clé d'authentification d'agent.

6. Entrez la clé d'authentification à utiliser pour l'installation de l'agent ou prenez note de l'entrée actuelle.

   Important : N'oubliez pas cette clé ou notez sa valeur. Vous en aurez besoin pour installer l'agent.



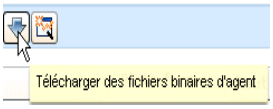
7. Cliquez sur Enregistrer.
8. Passez à l'étape suivante, Téléchargement du programme d'installation de l'agent.

Téléchargement du programme d'installation de l'agent

Si vous venez de définir la clé d'authentification de l'agent, vous êtes prêt à télécharger le programme d'installation de l'agent sur le bureau.

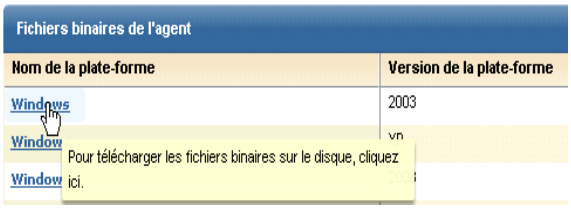
Pour télécharger le programme d'installation de l'agent

1. Dans la barre d'outils affichée pour l'Explorateur d'agent, cliquez sur Télécharger des fichiers binaires d'agent.



   Des liens vers les fichiers binaires d'agents disponibles apparaissent dans le volet principal.

2. Cliquez sur le lien Windows pour installer l'agent sur un serveur exécutant le système d'exploitation Windows Server 2003.


Fichiers binaires de l'agent
Nom de la plate-forme
Version de la plate-forme
Windows
2003
Pour télécharger les fichiers binaires sur le disque, cliquez ici.

   La boîte de dialogue Sélection de l'emplacement de téléchargement par <adresse IP> apparaît.

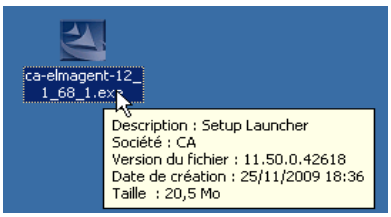
3. Sélectionnez le bureau, puis cliquez sur Enregistrer.

   Un message indiquant la progression du téléchargement du fichier binaire d'agent sélectionné apparaît, suivi d'un message de confirmation.

4. Cliquez sur OK.

5. Réduisez le navigateur mais laissez la connexion ouverte, afin de pouvoir vérifier rapidement l'installation une fois celle-ci terminée.

   Le lanceur du programme d'installation de l'agent apparaît sur le bureau.



Installation d'un agent

Avant de commencer, gardez à disposition les informations ci-dessous.

- Adresse IP du serveur CA Enterprise Log Manager à partir duquel vous avez téléchargé le programme de l'agent
- Nom et mot de passe du compte d'utilisateur que vous avez créé pour l'agent
- Clé d'authentification de l'agent que vous avez définie

Pour installer un agent destiné à un hôte Windows

1. Double-cliquez sur le lanceur de l'installation de l'agent.

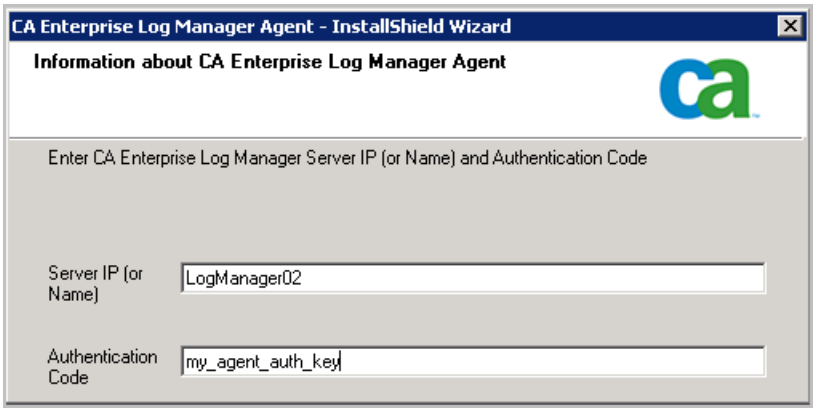
   L'assistant d'installation démarre.

2. Cliquez sur Suivant, lisez la licence, cliquez sur J'accepte les termes des contrats de licence pour continuer, puis cliquez sur Suivant.
3. Acceptez le chemin d'installation ou modifiez-le, puis cliquez sur Suivant.
4. Entrez les informations requises, comme suit.
   a. Entrez le nom d'hôte du CA Enterprise Log Manager auquel cet agent doit transférer les journaux qu'il collecte.

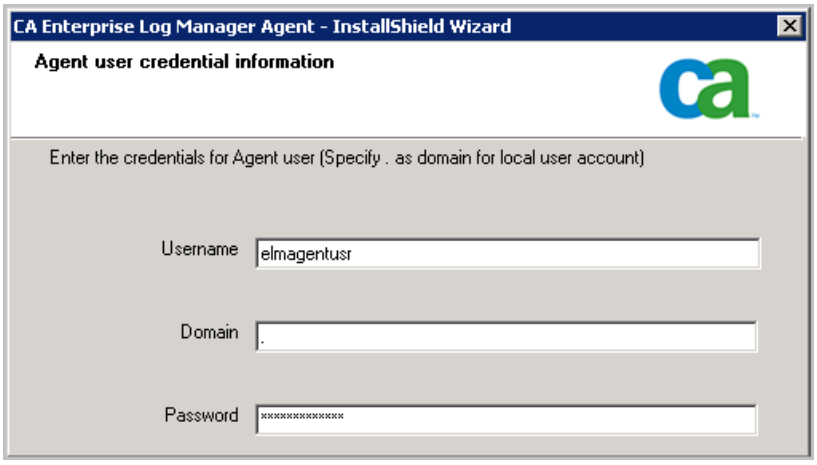
      Remarque : Comme CA Enterprise Log Manager de cet exemple de scénario utilise DHCP pour l'affectation des adresses IP, vous ne devez pas entrer d'adresse IP ici ; en effet, en cas de changement ultérieur de l'adresse IP du serveur, vous risqueriez de devoir réinstaller l'agent.

   b. Entrez la clé d'authentification de l'agent.

   Voici un exemple.


CA Enterprise Log Manager Agent - InstallShield Wizard
Information about CA Enterprise Log Manager Agent
Enter CA Enterprise Log Manager Server IP (or Name) and Authentication Code
Server IP (or Name)
LogManager02
Authentication Code
my_agent_auth_key

5. Entrez le nom et mot de passe du compte d'utilisateur que vous avez configuré pour l'agent, puis cliquez sur Suivant.



6. Cliquez sur Suivant. La spécification d'un fichier de connecteur exporté est facultative.

   La page Lancer la copie des fichiers apparaît.

7. Cliquez sur Suivant.

   Le processus d'installation de l'agent prend fin.

8. Cliquez sur Terminer.

9. Vous devez ensuite configurer des connecteurs pour cet agent.

   Une fois les connecteurs configurés, les événements collectés sont envoyés au magasin de journaux d'événements CA Enterprise Log Manager via le port 17001.

   Important : Si vous n'autorisez pas de trafic sortant à partir de l'hôte sur lequel vous avez installé l'agent et si vous utilisez le pare-feu Windows, vous devez ouvrir ce port sur ce pare-feu.

Informations complémentaires :

Téléchargement du programme d'installation de l'agent (page 37)
Création d'un compte d'utilisateur pour l'agent (page 35)
Définition de la clé d'authentification d'un agent (page 36)

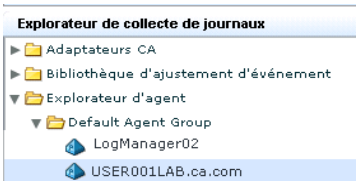
Création d'un connecteur basé sur NTEventLog

Après avoir installé un agent, vous créez un connecteur pour spécifier les sources des événements que vous souhaitez collecter. Votre agent étant installé sur un serveur Windows, vous devez créer un connecteur basé sur l'intégration NTEventLog et spécifier les paramètres du WMILogSensor, comme décrit dans le manuel du connecteur que vous ouvrez à partir de l'assistant de création d'un connecteur. Spécifiez le nom de l'hôte sur lequel l'agent est installé pour la collecte de journaux avec agent. Si vous le souhaitez, vous pouvez ajouter un autre détecteur de journaux WMI pour ce connecteur et spécifier un autre hôte que celui sur lequel l'agent est installé. Cela permet la collecte de journaux sans agent. Le ou les hôtes supplémentaires doivent se trouver dans le même domaine et disposer du même administrateur Windows que le premier hôte que vous avez ajouté.

Pour configurer un connecteur basé sur NTEventLog

1. Agrandissez votre navigateur affichant l'Explorateur d'agent CA Enterprise Log Manager.
2. Développez l'Explorateur d'agent, puis le groupe d'agents par défaut.

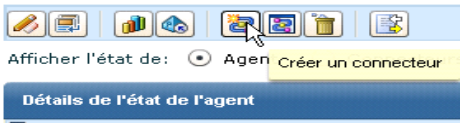
   Le nom de l'ordinateur sur lequel vous avez installé l'agent apparaît.

3. Sélectionnez cet agent.

   Le volet Connecteurs de l'agent apparaît.

4. Cliquez sur Créer un connecteur.

   L'assistant de création d'un connecteur apparaît ; l'étape Détails du connecteur est sélectionnée.

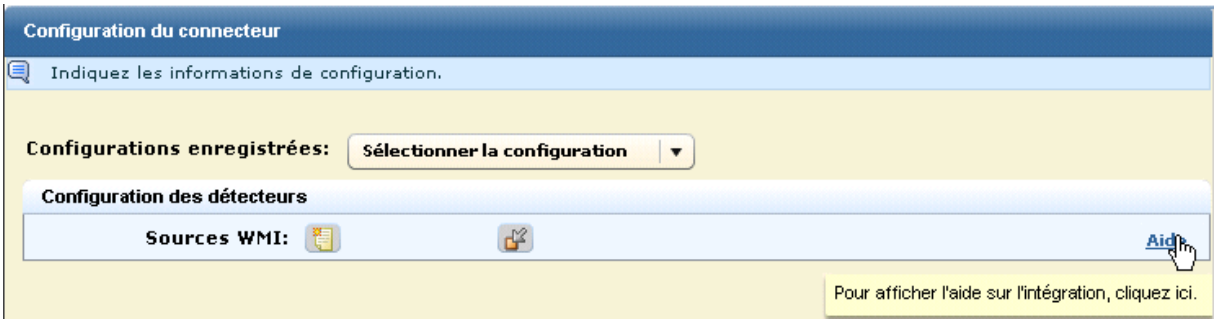
5. Laissez Intégrations sélectionné, puis sélectionnez NTEventLog dans la liste déroulante Intégration.

   Les champs Nom du connecteur et Description sont remplis selon la sélection effectuée dans Intégration.

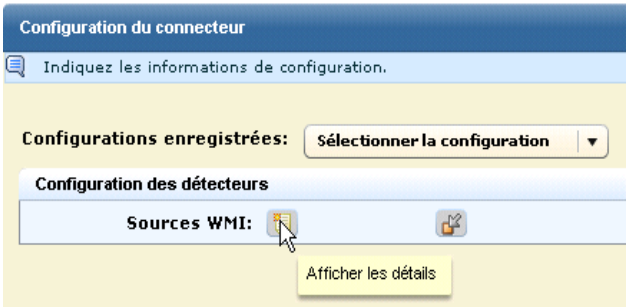
6. Modifiez le nom du connecteur afin d'obtenir un nom unique. Vous pouvez envisager de compléter ce nom par le nom du serveur cible, par exemple NTEventLog_Connector_USER001LAB.

7. Sélectionnez l'étape Configuration du connecteur.

Le volet Configuration des détecteurs apparaît ; un bouton Aide permet d'accéder au manuel du connecteur NTEventLog qui décrit les champs de configuration du détecteur.

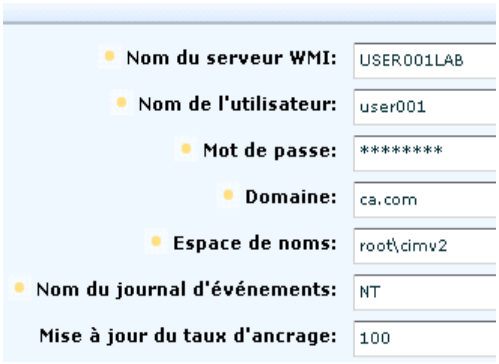


8. Cliquez sur le bouton Afficher les détails pour les sources WMI.



9. Configurez les paramètres WMILogSensor pour l'ordinateur local de collecte de journaux avec agent. Pour plus de détails, cliquez sur le lien Aide.

   Les exemples ci-après présentent une configuration où l'utilisateur est un administrateur Windows sur le serveur WMI spécifié. Le domaine est défini pour le serveur WMI.



10. Configurez un détecteur WMI pour un autre ordinateur, pour une collecte de journaux sans agent utilisant ce même connecteur (facultatif).

    a. Cliquez sur le bouton Répéter le supernoeud.

       L'illustration suivante présente une configuration comportant deux sources WMI.

    b. Configurez les paramètres WMILogSensor pour un autre ordinateur.

    L'exemple ci-après présente une configuration pour un deuxième détecteur de journaux WMI dans le même domaine et avec les mêmes informations d'identification d'administrateur.

11. Cliquez sur Enregistrer et fermer.

12. Pour afficher l'état du connecteur que vous avez configuré, procédez comme suit.

    a. Sélectionnez l'agent dans le volet gauche.

    b. Cliquez sur Etat et commande.

    c. Sélectionnez Afficher l'état des connecteurs.

    Le volet Détails de l'état apparaît.

13. Cliquez sur le lien Exécution en cours.

    L'état affiché de la cible configurée dans le connecteur inclut le pourcentage d'UC, l'utilisation de la mémoire et le nombre moyen d'événements par seconde.

Configuration d'une source d'événement Windows

Après avoir configuré un connecteur à l'aide de l'intégration NTEventLog sur l'agent, vous devez pouvoir consulter des événements au moyen de la visionneuse d'événements. Si des événements ne sont pas transférés à votre visionneuse, vous devez modifier les paramètres Windows de vos stratégies locales sur la source d'événement.

Pour configurer des stratégies locales sur la source d'événement d'un connecteur NTEventLog

1. Si l'explorateur de collecte de journaux n'est pas déjà affiché, cliquez sur l'onglet Administration.
2. Développez Bibliothèque d'ajustement d'événement, Intégrations, Abonnement, puis sélectionnez NTEventLog et cliquez sur le lien Aide situé au-dessus du nom de l'intégration dans le volet Afficher les détails de l'intégration.

   Le manuel du connecteur pour le journal d'événements NT (sécurité, application, système) apparaît.

3. Réduisez l'interface utilisateur CA Enterprise Log Manager, puis suivez les indications du manuel du connecteur pour modifier les stratégies locales sur une source d'événement s'exécutant sous Windows.

   Remarque : Si vous utilisez Windows Server 2003, sélectionnez Panneau de configuration, Outils d'administration, Stratégie de sécurité locale, puis développez Stratégies locales.

4. Si vous avez configuré un détecteur WMI pour un second serveur WMI, modifiez également les stratégies locales de ce serveur (facultatif).
5. Agrandissez CA Enterprise Log Manager.

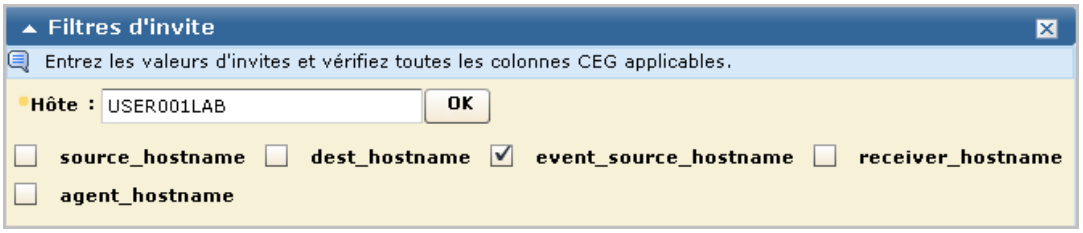
Affichage de journaux à partir de sources d'événement Windows

Pour afficher rapidement les résultats d'une requête sur des événements collectés par un écouteur Syslog, utilisez l'invite Hôte. Vous pouvez également sélectionner des requêtes ou des rapports.

Pour afficher les journaux d'événements entrants

1. Sélectionnez l'onglet Requêtes et rapports.

   Le sous-onglet Requêtes s'affiche.
2. Développez Invites sous Liste de requêtes, puis sélectionnez Hôte.
3. Dans le champ Hôte, entrez le nom du serveur WMI configuré pour le détecteur. Désélectionnez les autres cases, puis cliquez sur OK.

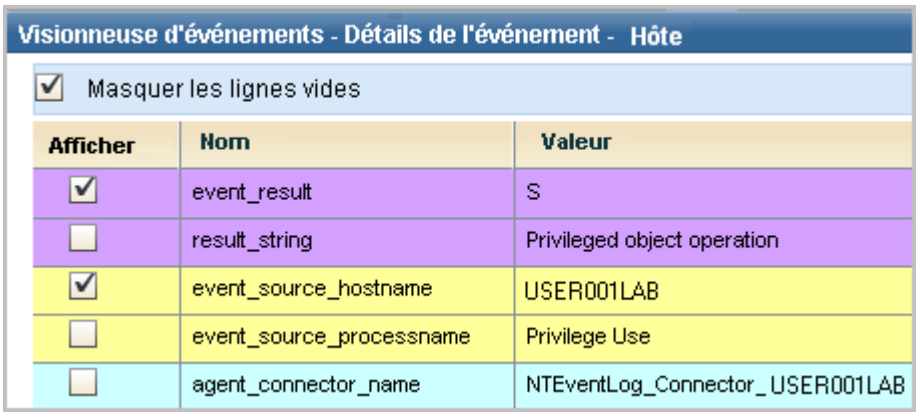


   Les événements provenant des sources d'événement du serveur WMI apparaissent.
4. Cliquez sur Sévérité CA, puis faites défiler pour rechercher un avertissement. L'exemple ci-dessous est compressé, sans les colonnes Date et Source d'événement.

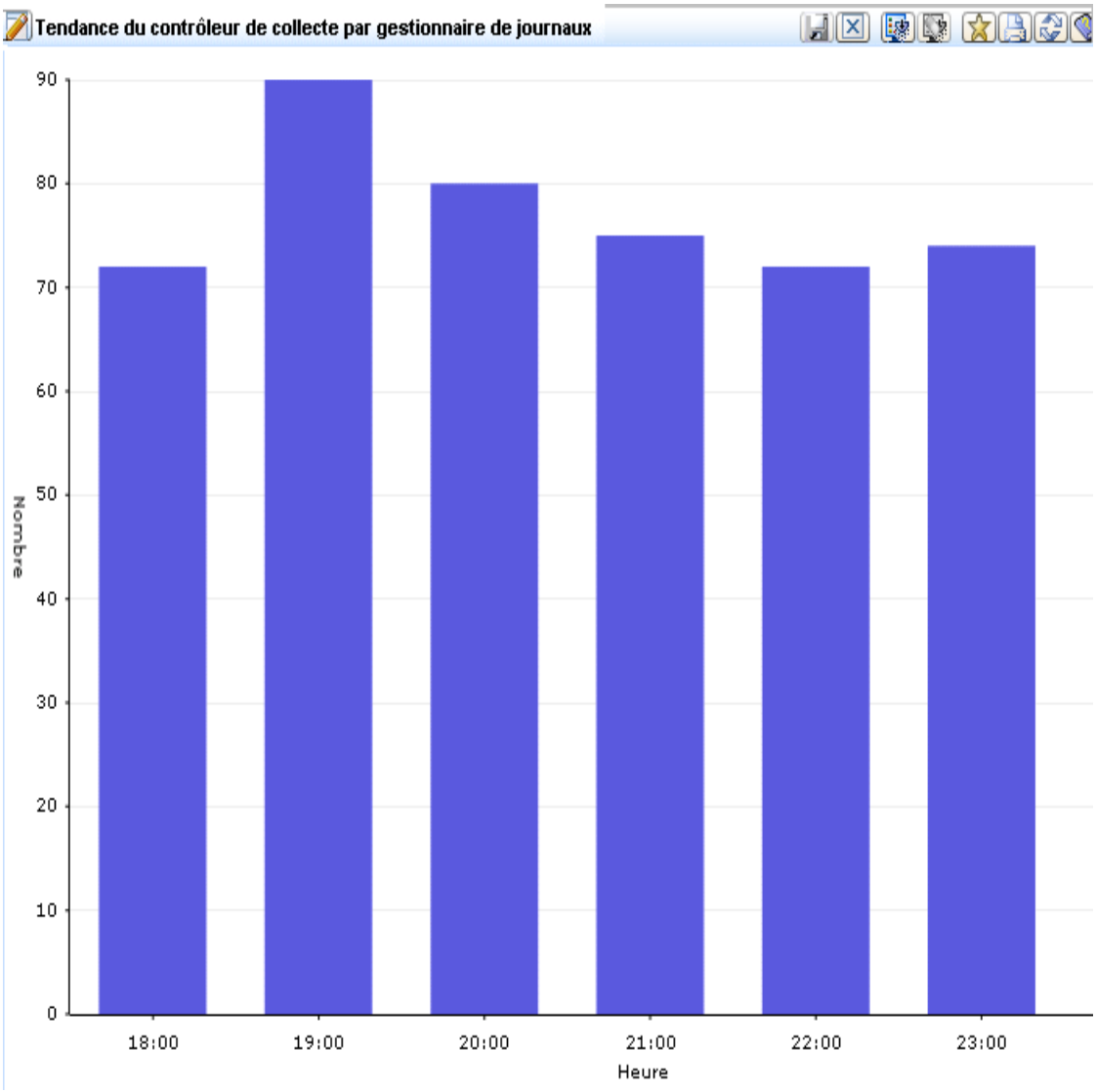
Sévérité CA ▼	Utilisateur de	Résultat	Catégorie	Action	Nom du journal
Warning	calm_agent	S	System Access	Privilege Use	NT-Security

5. Cliquez sur Afficher les événements bruts pour afficher les événements bruts de l'avertissement.

6. Double-cliquez sur l'avertissement pour afficher la visionneuse d'événements avec beaucoup plus de données. Quelques lignes d'exemples de données sont affichées ci-dessous.



7. Cliquez sur l'onglet Requêtes et rapports, cliquez sur une requête de la liste de requêtes, par exemple Tendance du contrôleur de collecte par gestionnaire de journaux. Affichez le graphique à barres des résultats.



8. Cliquez sur Rapports. Sous Liste de rapports, entrez auto dans le champ Rechercher, afin d'afficher le nom du rapport Evénements d'autosurveillance du système. Sélectionnez ce rapport pour afficher une liste des événements générés par le serveur CA Enterprise Log Manager.

Remarque : Pour obtenir des détails concernant la planification de rapports sur les informations que vous souhaitez analyser, consultez l'aide en ligne ou le *Manuel d'administration*.

Chapitre 4 : Principales fonctionnalités

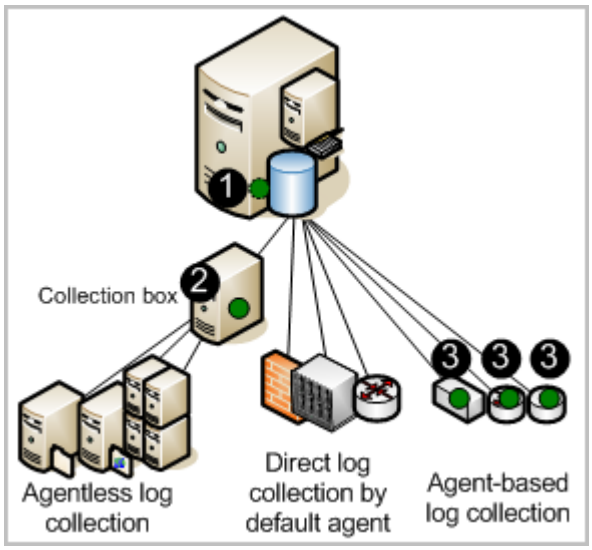
Ce chapitre traite des sujets suivants :

Collecte de journaux (page 49)
Stockage des journaux (page 51)
Présentation normalisée des journaux (page 53)
Génération de rapports de conformité (page 54)
Alerte de violation de stratégie (page 56)
Gestion des droits (page 57)
Accès selon un rôle (page 58)
Gestion de l'abonnement (page 59)
Contenu prêt à l'emploi (page 60)

Collecte de journaux

Le serveur CA Enterprise Log Manager peut être configuré pour collecter des journaux à l'aide d'une ou de plusieurs techniques prises en charge. Les techniques diffèrent quant au type et à l'emplacement du composant qui écoute et collecte les journaux. Ces composants sont configurés sur les agents.

L'illustration ci-dessous décrit un système avec un seul serveur, où l'emplacement des agents est indiqué par un cercle sombre (vert).



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Configurez l'agent par défaut sur CA Enterprise Log Manager pour récupérer directement des événements auprès des sources Syslog spécifiées.
2. Configurez l'agent installé sur un point de collecte Windows pour collecter des événements provenant des serveurs Windows spécifiés et les transmettre à CA Enterprise Log Manager.
3. Configurez les agents installés sur des hôtes où sont exécutées les sources d'événement, pour collecter le type d'événement configuré et effectuer la suppression.

Remarque : Le trafic entre l'agent et le serveur CA Enterprise Log Manager de destination est toujours chiffré.

Etudiez les avantages de chaque technique de collecte de journaux ci-dessous.

- Collecte directe de journaux

  Avec la collecte directe de journaux, vous configurez l'écouteur Syslog sur l'agent par défaut pour recevoir les événements des sources fiables spécifiées. Vous pouvez également configurer d'autres connecteurs pour collecter des événements provenant de n'importe quelle source d'événement compatible avec l'environnement de fonctionnement du dispositif logiciel.

  Avantage : vous n'avez pas besoin d'installer un agent pour collecter les journaux des sources d'événement à proximité du serveur CA Enterprise Log Manager sur le réseau.

- Collecte sans agent

  Avec la collecte sans agent, il n'existe aucun agent local sur les sources d'événement. Au lieu de cela, un agent est installé sur un point de collecte dédié. Des connecteurs sont configurés pour chaque source d'événement cible sur cet agent.

  Avantage : vous pouvez collecter des journaux provenant de sources d'événement s'exécutant sur des serveurs où vous ne pouvez pas installer d'agents, comme des serveurs où la stratégie d'entreprise interdit les agents. La remise est garantie, par exemple, lorsque la collecte de journaux ODBC est correctement configurée.

- Collecte avec agent

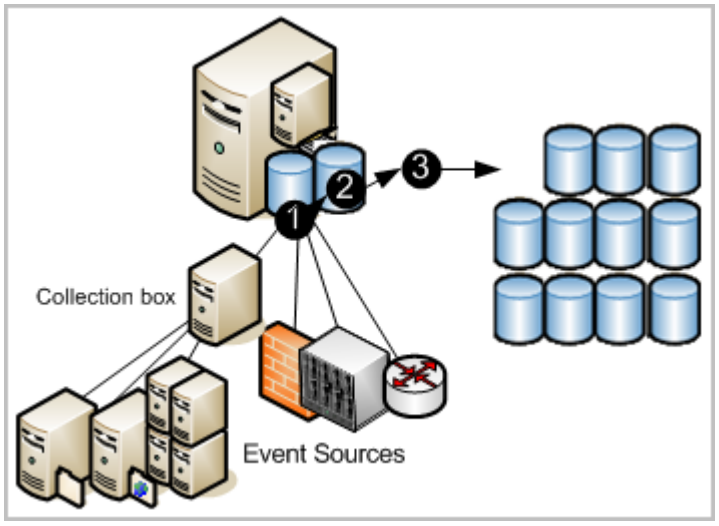
  Pour la collecte avec agent, un agent est installé lorsqu'une ou plusieurs sources d'événement sont exécutées et qu'un connecteur est configuré pour chaque source d'événement.

  Avantage : vous pouvez collecter des journaux provenant d'une source pour laquelle la bande passante du réseau vers CA Enterprise Log Manager n'est pas suffisamment efficace pour prendre en charge la collecte directe de journaux. Vous pouvez utiliser l'agent pour filtrer les événements et réduire le trafic émis sur le réseau. La remise d'événement est garantie.

Remarque : Pour plus de détails sur la configuration des agents, consultez le *Manuel d'administration*.

Stockage des journaux

CA Enterprise Log Manager dispose du stockage intégré et géré des journaux des bases de données récemment archivées. Les événements collectés par les agents provenant de sources d'événement suivent un cycle de stockage tel qu'illustré par le schéma ci-dessous.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Les nouveaux événements collectés par n'importe quelle technique sont envoyés à CA Enterprise Log Manager. L'état des événements entrants dépend de la technique utilisée pour les collecter. Les événements entrants doivent être ajustés avant d'être insérés dans la base de données.
2. Lorsque la base de données des enregistrements ajustés atteint la taille configurée, tous les enregistrements sont compressés en une base de données et enregistrés sous un seul nom. La compression des données des journaux réduit les coûts induits par leur déplacement et leur stockage. La base de données compressée peut être déplacée automatiquement en fonction de la configuration de l'archivage automatique ; vous pouvez également la sauvegarder et la déplacer manuellement avant qu'elle n'atteigne la durée configurée avant suppression (les bases de données archivées automatiquement sont supprimées de la source dès qu'elles sont déplacées).
3. Si vous configurez l'archivage automatique pour qu'il déplace chaque jour les bases de données compressées vers un serveur distant, vous pouvez déplacer ces sauvegardes vers un stockage de journaux hors site à long terme si vous le souhaitez. En conservant les sauvegardes des journaux, vous respectez les réglementations stipulant que les journaux doivent être collectés de manière sécurisée, stockés de manière centralisée pendant un certain nombre d'années et disponibles pour être examinés (vous pouvez restaurer la base de données à tout moment depuis le stockage à long terme).

Remarque : Pour plus de détails sur la configuration du magasin de journaux d'événements, y compris la configuration de l'archivage automatique, consultez le *Manuel d'implémentation*. Pour plus de détails sur la restauration des sauvegardes à des fins d'examen et de génération de rapports, consultez le *Manuel d'administration*.

Présentation normalisée des journaux

Les journaux générés par les applications, les systèmes d'exploitation et les unités utilisent tous leur propre format. CA Enterprise Log Manager ajuste les journaux collectés afin de normaliser la consignation des données. Le format standard facilite la comparaison des données collectées auprès de différentes sources pour les auditeurs et les cadres supérieurs. Techniquement, le CEG (Common Event Grammar) CA facilite l'implémentation de la normalisation et de la classification des événements.

La CEG propose plusieurs champs utilisés pour normaliser différents aspects de l'événement, notamment ceux répertoriés ci-dessous.

- Modèle idéal (classe de technologies comme les antivirus, les SGBD et les pare-feu)
- Catégorie (par exemple Gestion des identités et Sécurité du réseau)
- Classe (par exemple Gestion des comptes et Gestion de groupes)
- Action (par exemple Création d'un compte et Création d'un groupe)
- Résultats (par exemple Opération réussie et Echec)

Remarque : Pour plus de détails sur les règles et fichiers utilisés lors de l'ajustement des événements, consultez le *Manuel d'administration CA Enterprise Log Manager*. Consultez la section relative à la Grammaire commune aux événements dans l'aide en ligne pour de plus amples détails sur la normalisation et la classification des événements.

Génération de rapports de conformité

CA Enterprise Log Manager vous permet de collecter et de traiter des données relatives à la sécurité, puis de les transformer en rapports appropriés pour les auditeurs internes ou externes. Vous pouvez interagir par le biais de requêtes et de rapports à des fins d'examen. Vous pouvez automatiser le processus de génération de rapports en planifiant les jobs de rapport.

Le système offre les avantages ci-dessous.

- Simplicité de formulation de requêtes, grâce aux balises
- Génération de rapports en temps quasi-réel
- Centralisation de la recherche dans les archives distribuées des journaux critiques

Il se concentre sur la génération de rapports de conformité plutôt que sur la corrélation en temps réel des événements et alertes. La réglementation exige la génération de rapports prouvant la conformité avec les contrôles relatifs au secteur. CA Enterprise Log Manager fournit des rapports contenant les balises ci-dessous pour faciliter l'identification.

- Basel II
- COBIT
- COSO
- Directive UE - Protection des données
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Vous pouvez examiner des rapports de journaux prédéfinis ou effectuer des recherches en fonction de critères spécifiés par vos soins. De nouveaux rapports sont fournis avec les mises à jour d'abonnement.

Les fonctionnalités d'affichage des journaux reposent sur les éléments suivants :

- Requêtes à la demande, prédéfinies ou définies par l'utilisateur, dont les résultats peuvent atteindre jusqu'à 5 000 enregistrements
- Recherche rapide, au moyen d'invites, pour un nom d'hôte, une adresse IP, un numéro de port ou un nom d'utilisateur spécifié
- Génération de rapports planifiée et à la demande, avec contenu de génération de rapports prêt à l'emploi
- Requêtes et alertes planifiées
- Rapports de base avec informations de tendances
- Visionneuses d'événements interactives et graphiques
- Génération automatisée de rapport avec pièce jointe de courriel
- Stratégies de conservation automatisée de rapport

Remarque : Pour plus de détails sur l'utilisation de requêtes et de rapports prédéfinis ou sur la création de requêtes et de rapports personnalisés, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Alerte de violation de stratégie

CA Enterprise Log Manager vous permet d'automatiser l'envoi d'un courriel d'alerte lorsque survient un événement qui nécessite une attention à court terme. Vous pouvez également surveiller à tout instant les alertes d'action à partir de CA Enterprise Log Manager, en spécifiant un intervalle de temps, depuis les cinq dernières minutes jusqu'aux 30 derniers jours écoulés. Des alertes sont envoyées automatiquement à un flux RSS auquel il est possible d'accéder à partir d'un navigateur Web. Si vous le souhaitez, vous pouvez spécifier d'autres destinations, y compris des adresses électroniques, un processus CA IT PAM, qui génère des tickets de bureau d'assistance, et une ou plusieurs adresses IP de destination d'interruption SNMP.

Pour vous aider à commencer, de nombreuses requêtes prédéfinies sont disponibles pour être planifiées, sans modification, en alertes d'action. Quelques exemples sont présentés ci-dessous.

- Activité excessive de l'utilisateur
- Utilisation élevée de l'UC
- Peu d'espace disque disponible
- Journal des événements de sécurité effacé au cours des dernières 24 heures
- Stratégie d'audit Windows modifiée au cours des dernières 24 heures

Certaines requêtes comportent des listes à clés, où vous fournissez les valeurs utilisées par la requête. Certaines listes à clés contiennent des valeurs prédéfinies que vous pouvez compléter, par exemple les comptes par défaut et les groupes avec droits. D'autres listes à clés, comme celle des ressources stratégiques, ne comportent pas de valeurs par défaut. Une fois configurées, des alertes peuvent être planifiées pour des requêtes prédéfinies comme celles répertoriées ci-dessous.

- Ajout ou retrait d'une appartenance à un groupe par des groupes avec droits.
- Connexion établie par le compte par défaut
- Aucun événement reçu par les sources stratégiques.

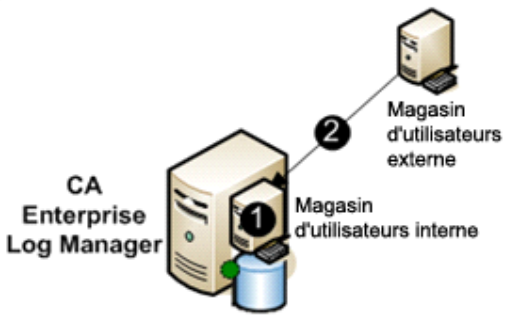
Les listes à clés peuvent être mises à jour manuellement, en important un fichier, ou en exécutant un traitement des valeurs dynamiques de CA IT PAM.

Remarque : Pour plus de détails sur les alertes d'action, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Gestion des droits

Lorsque vous configurez le magasin d'utilisateurs, vous pouvez utiliser le magasin d'utilisateurs par défaut sur CA Enterprise Log Manager pour configurer des comptes d'utilisateur ou référencer un magasin d'utilisateurs externe contenant des comptes d'utilisateur déjà définis. La base de données sous-jacente est exclusive à CA Enterprise Log Manager et n'utilise pas un SGBD du commerce.

Les magasins d'utilisateurs externes pris en charge incluent CA SiteMinder et les répertoires LDAP comme Microsoft Active Directory, Sun One et Novell eDirectory. Si vous faites référence à un magasin d'utilisateurs externe, les informations des comptes d'utilisateur sont automatiquement chargées en lecture seule, tel qu'illustré par la flèche dans le schéma ci-dessous. Vous définissez uniquement les détails propres à l'application pour les comptes sélectionnés. Aucune donnée n'est déplacée du magasin d'utilisateurs interne vers le magasin d'utilisateurs externe référencé.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Le magasin d'utilisateurs interne procède à la gestion des droits en authentifiant les informations d'identification fournies par les utilisateurs lors de la connexion et en autorisant l'accès des utilisateurs aux différentes fonctions de l'interface utilisateur, en fonction des stratégies associées aux rôles affectés à leurs comptes d'utilisateur. Si le nom d'utilisateur et le mot de passe d'un utilisateur tentant de se connecter ont été chargés par un magasin d'utilisateurs externe, les informations d'identification entrées doivent correspondre aux informations d'identification chargées.
2. La seule fonction du magasin d'utilisateurs externe consiste à charger ses comptes d'utilisateur dans le magasin d'utilisateurs interne. Ces comptes sont chargés automatiquement lorsque la référence au magasin d'utilisateurs est enregistrée.

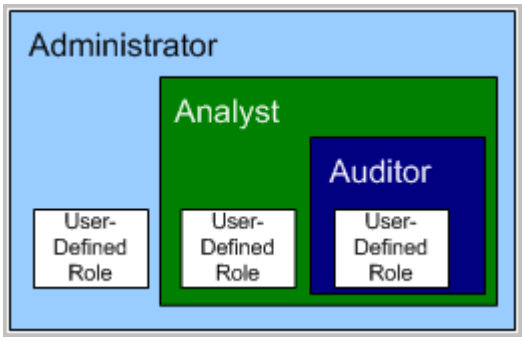
Remarque : Pour plus de détails sur la configuration de l'accès de l'utilisateur de base, consultez le *Manuel d'implémentation CA Enterprise Log Manager*. Pour plus de détails sur les stratégies de prise en charge de rôles prédéfinis, de création de comptes d'utilisateur et d'affectation de rôles, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Accès selon un rôle

CA Enterprise Log Manager propose trois groupes d'applications ou rôles prédéfinis. Les administrateurs affectent les rôles ci-dessous aux utilisateurs, pour spécifier leurs droits d'accès aux fonctions CA Enterprise Log Manager.

- Administrator
- Analyst
- Auditor

L'auditeur peut accéder à quelques fonctions. L'analyste peut accéder à toutes les fonctions Auditor, auxquelles s'ajoutent quelques autres fonctions. L'administrateur peut accéder à toutes les fonctions. Vous pouvez définir un rôle personnalisé avec des stratégies associées qui limitent l'accès de l'utilisateur aux ressources, de façon à répondre à vos besoins commerciaux.



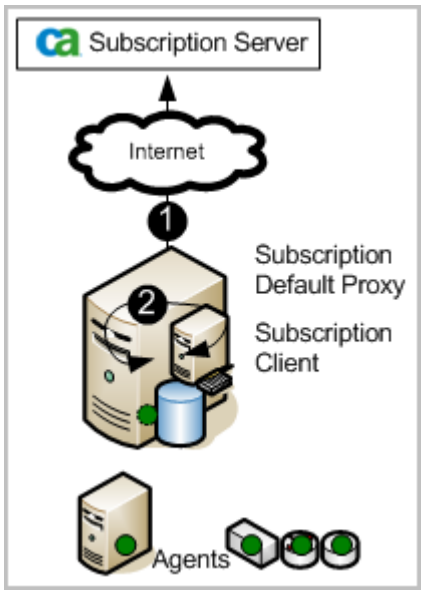
Les administrateurs peuvent personnaliser l'accès à n'importe quelle ressource en créant un groupe d'applications personnalisé avec des stratégies associées, puis en affectant ce groupe d'applications, ou rôle, aux comptes d'utilisateur.

Remarque : Pour plus de détails sur la planification et la création de rôles personnalisés, de stratégies personnalisées et de filtres d'accès, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Gestion de l'abonnement

Le module d'abonnement est le service qui permet de télécharger automatiquement, de manière planifiée, les mises à jour d'abonnement provenant du serveur d'abonnement CA et de les distribuer aux serveurs CA Enterprise Log Manager. Lorsqu'une mise à jour d'abonnement inclut le module pour les agents, les utilisateurs lancent le déploiement de ces mises à jour vers les agents. *Les mises à jour d'abonnement* sont des mises à jour de composants CA Enterprise Log Manager, ainsi que des mises à jour de système d'exploitation, des correctifs et des mises à jour de contenu, comme les rapports.

L'illustration ci-dessous décrit le scénario le plus simple de connexion directe à Internet.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Le serveur CA Enterprise Log Manager, en tant que serveur d'abonnements par défaut, contacte le serveur d'abonnements CA concernant les mises à jour et télécharge toute mise à jour nouvellement disponible. Le serveur CA Enterprise Log Manager crée une sauvegarde, puis envoie les mises à jour de contenu vers le composant incorporé du serveur de mises à jour qui stocke les mises à jour de contenu pour tous les autres serveurs CA Enterprise Log Manager.
2. En tant que client d'abonnement, le serveur CA Enterprise Log Manager installe lui-même les mises à jour des produits et du système d'exploitation dont il a besoin.

Remarque : Pour plus de détails sur la planification et la configuration de l'abonnement, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'ajustement et la modification de la configuration d'abonnement et sur l'application des mises à jour aux agents, consultez le *Manuel d'administration*.

Contenu prêt à l'emploi

CA Enterprise Log Manager contient un contenu prédéfini que vous commencez à utiliser dès l'installation et la configuration du produit. Le processus d'abonnement ajoute régulièrement du contenu nouveau et met à jour celui existant.

Les catégories de contenu prédéfini incluent :

- Rapports avec balises
- Requêtes avec balises
- Intégrations avec des capteurs associés, fichiers d'analyse (XMP), fichiers de mappage (DM) et, dans certains cas, règles de suppression
- Règles de suppression et de récapitulation

Chapitre 5 : Informations complémentaires concernant CA Enterprise Log Manager

Ce chapitre traite des sujets suivants :

Affichage des infobulles (page 61)
Affichage de l'aide en ligne (page 63)
Exploration de la bibliothèque de documentation (page 65)

Affichage des infobulles

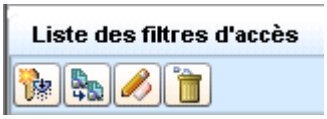
Vous pouvez identifier la finalité des boutons, des cases à cocher et des rapports de la page CA Enterprise Log Manager dans votre affichage actuel.

Pour afficher les infobulles et autres aides

1. Déplacez votre curseur au-dessus des boutons pour afficher la description de leur fonction. Vous pouvez ainsi visualiser la fonction de n'importe quel bouton.

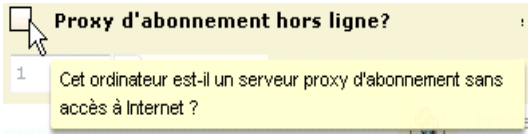
2. Notez la différence entre les boutons actifs et inactifs.

   Lorsqu'ils sont activés, les boutons s'affichent en couleur. Par exemple, le bouton Liste des filtres d'accès s'affiche en couleur pour les administrateurs de la gestion des utilisateurs et des accès.

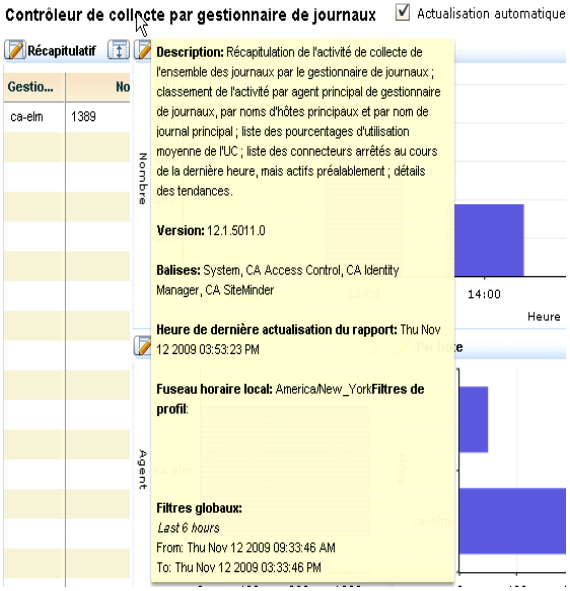


Lorsqu'ils sont désactivés, les boutons s'affichent en noir et blanc. Par exemple, les boutons Liste des filtres d'accès s'affichent en noir et blanc pour les auditeurs.

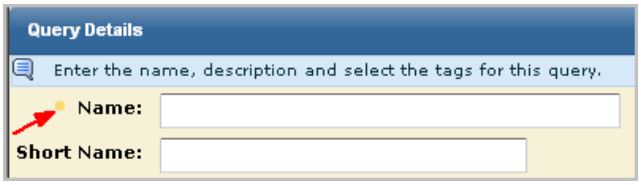
3. Affichez les descriptions des champs de saisie ou des cases à cocher en déplaçant votre curseur au-dessus du nom du champ.



4. Affichez les descriptions des rapports en déplaçant votre curseur au-dessus du nom du rapport.


Contrôleur de collecte par gestionnaire de journaux
Actualisation automatique
Récapitulatif
Description: Récapitulation de l'activité de collecte de l'ensemble des journaux par le gestionnaire de journaux ; classement de l'activité par agent principal de gestionnaire de journaux, par noms d'hôtes principaux et par nom de journal principal ; liste des pourcentages d'utilisation moyenne de l'UC ; liste des connecteurs arrêtés au cours de la dernière heure, mais actifs préalablement ; détails des tendances.
Version: 12.1.5011.0
Balises: System, CA Access Control, CA Identity Manager, CA SiteMinder
Heure de dernière actualisation du rapport: Thu Nov 12 2009 03:53:23 PM
Fuseau horaire local: America/New_YorkFiltres de profil:
Filtres globaux:
Last 6 hours
From: Thu Nov 12 2009 09:33:46 AM
To: Thu Nov 12 2009 03:33:46 PM
Gestio...
No
ca-elm
1389
Nombre
Agent
14:00
Heure

5. Vous remarquerez un point orange à gauche de certains champs. Ce point signifie que le champ est obligatoire. Pour les configurations pouvant être enregistrées, vous ne pouvez pas effectuer d'enregistrement tant que tous les champs obligatoires ne sont pas renseignés.



Affichage de l'aide en ligne

Vous pouvez afficher de l'aide sur la page que vous consultez ou pour toute tâche que vous souhaitez effectuer.

Pour afficher l'aide en ligne

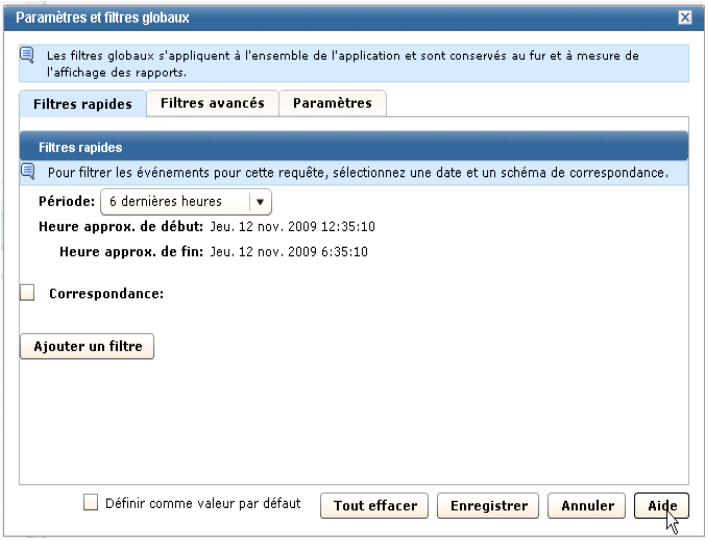
1. Cliquez sur le lien Aide dans la barre d'outils pour afficher le système d'aide en ligne de CA Enterprise Log Manager.

   Le système d'aide de CA Enterprise Log Manager apparaît, son contenu étant affiché dans le volet gauche.

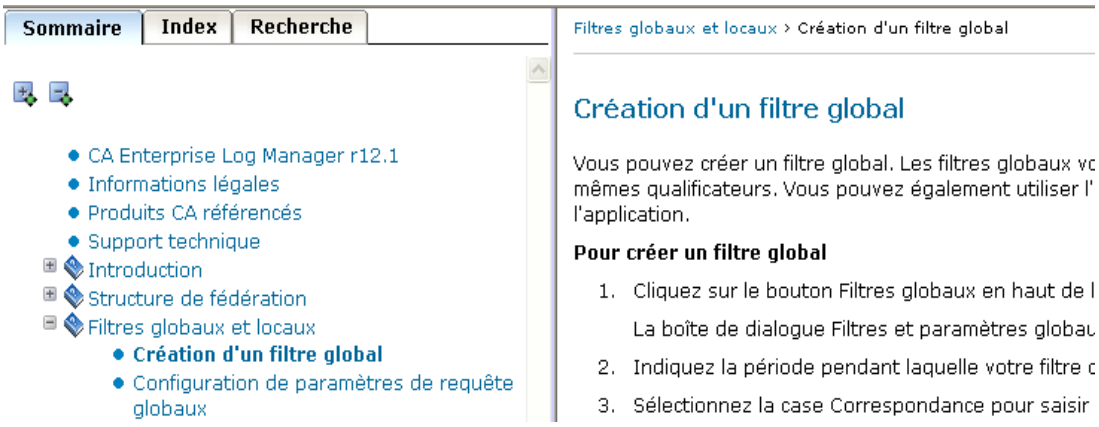
2. L'exemple ci-dessous présente l'accès à l'aide contextuelle à partir d'un bouton Aide.

   a. Cliquez sur le bouton Afficher/Modifier les filtres globaux.

La fenêtre Filtres et paramètres globaux apparaît et affiche un bouton Aide.


Paramètres et filtres globaux
Les filtres globaux s'appliquent à l'ensemble de l'application et sont conservés au fur et à mesure de l'affichage des rapports.
Filtres rapides
Filtres avancés
Paramètres
Filtres rapides
Pour filtrer les événements pour cette requête, sélectionnez une date et un schéma de correspondance.
Période:
6 dernières heures
Heure approx. de début: Jeu. 12 nov. 2009 12:35:10
Heure approx. de fin: Jeu. 12 nov. 2009 6:35:10
Correspondance:
Ajouter un filtre
Définir comme valeur par défaut
Tout effacer
Enregistrer
Annuler
Aide

b. Cliquez sur le bouton Aide. L'aide en ligne pour la procédure que vous pouvez effectuer sur la page, le volet ou la boîte de dialogue en cours apparaît dans une fenêtre secondaire.


Sommaire
Index
Recherche
CA Enterprise Log Manager r12.1
Informations légales
Produits CA référencés
Support technique
Introduction
Structure de fédération
Filtres globaux et locaux
Création d'un filtre global
Configuration de paramètres de requête globaux
Filtres globaux et locaux › Création d'un filtre global
Création d'un filtre global
Vous pouvez créer un filtre global. Les filtres globaux vc
mêmes qualificateurs. Vous pouvez également utiliser l'
l'application.
Pour créer un filtre global
1. Cliquez sur le bouton Filtres globaux en haut de l
La boîte de dialogue Filtres et paramètres globau
2. Indiquez la période pendant laquelle votre filtre c
3. Sélectionnez la case Correspondance pour saisir

c. Si vous savez quelle tâche effectuer sans connaître la méthode d'accès à la page correspondante dans CA Enterprise Log Manager, vous pouvez rechercher cette page dans la table des matières. Cliquez sur le titre de la tâche pour afficher la page correspondante.

Remarque : Si vous ne trouvez pas la tâche dont vous avez besoin dans la table des matières, consultez la bibliothèque de documentation.

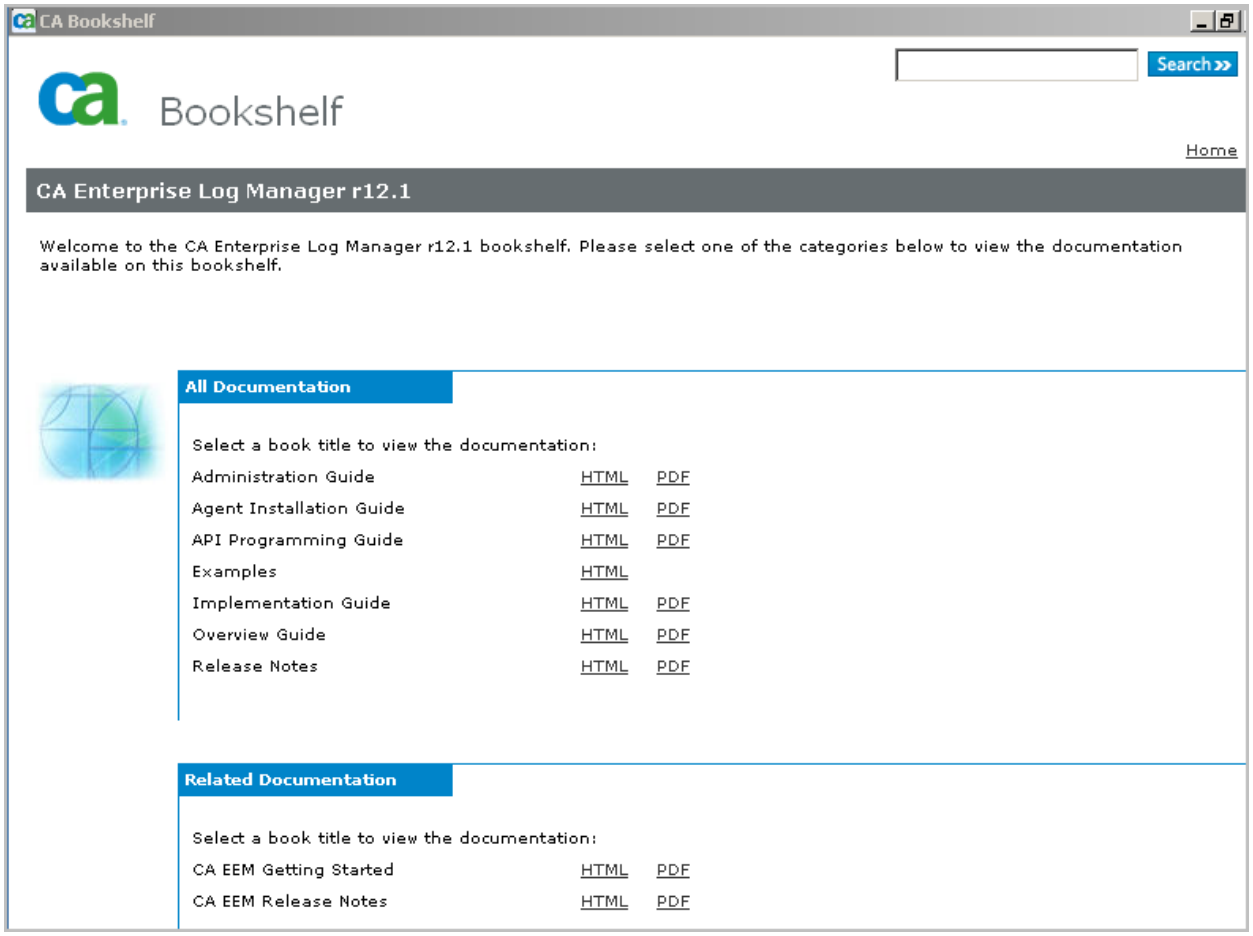
Exploration de la bibliothèque de documentation

Vous pouvez copier la bibliothèque sur votre lecteur local et ouvrir le livre souhaité au format HTML ou PDF. Les livres au format HTML contiennent des références croisées d'un livre à l'autre.

Pour explorer la bibliothèque

1. Copiez sur votre lecteur local la bibliothèque présente sur le DVD d'installation de l'application ou téléchargez-la à partir du site de support clientèle de CA. Pour ouvrir la bibliothèque, double-cliquez sur Bookshelf.hta ou sur Bookshelf.html.

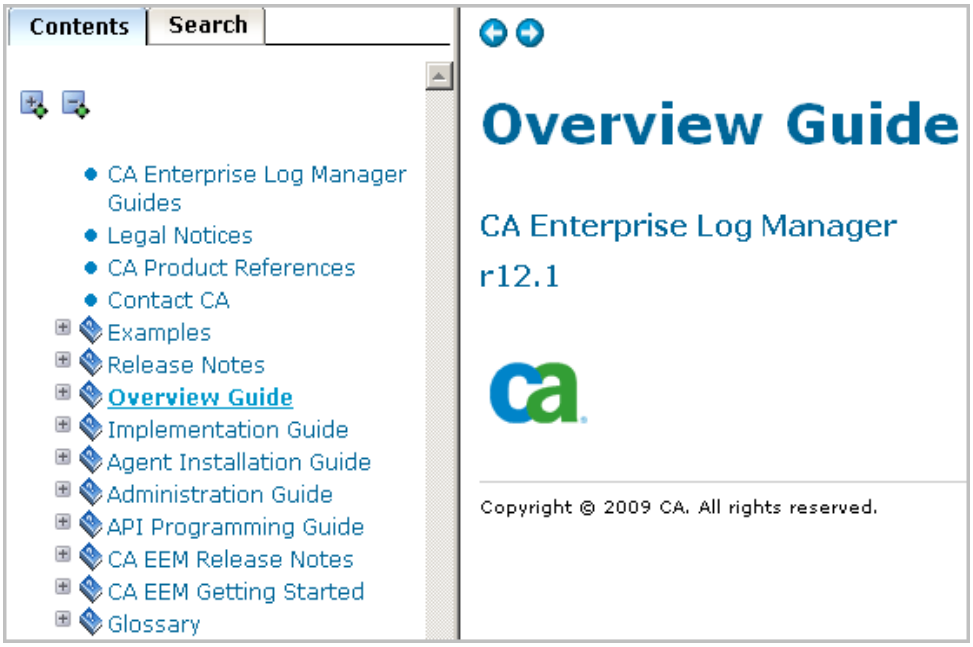
   Une page similaire à la page suivante apparaît.


CA Bookshelf
Search
Bookshelf
Home
CA Enterprise Log Manager r12.1
Welcome to the CA Enterprise Log Manager r12.1 bookshelf. Please select one of the categories below to view the documentation available on this bookshelf.
All Documentation
Select a book title to view the documentation:
Administration Guide HTML PDF
Agent Installation Guide HTML PDF
API Programming Guide HTML PDF
Examples HTML
Implementation Guide HTML PDF
Overview Guide HTML PDF
Release Notes HTML PDF
Related Documentation
Select a book title to view the documentation:
CA EEM Getting Started HTML PDF
CA EEM Release Notes HTML PDF

Le contenu des principaux manuels et des exemples est répertorié ci-dessous.

Produit livrable	Description
Manuel d'installation des agents	Installer des agents.
Manuel d'implémentation	Installer et configurer un système CA Enterprise Log Manager.
Manuel d'administration	Personnalisez la configuration, effectuez des tâches d'administration de routine et utilisez les requêtes, les rapports et les alertes.
Manuel de programmation de l'API	Utilisez l'API pour afficher des données d'événement dans un navigateur Web ou incorporer des rapports dans un autre produit CA ou tiers.
Exemples	Résoudre des problèmes professionnels courants, avec des liens vers des rubriques de la documentation.

2. Saisissez une valeur dans le champ d'entrée Rechercher, puis cliquez sur le bouton Rechercher pour afficher toutes les occurrences documentées qui comprennent votre entrée.
3. Cliquez sur un lien Imprimer pour ouvrir le PDF du manuel sélectionné.
4. Cliquez sur un lien HTML pour ouvrir l'ensemble de documentation intégré. Cet ensemble intégré comprend tous les manuels au format HTML. Si vous sélectionnez le lien HTML du Manuel de présentation, ce manuel est affiché.



Glossaire

accès aux données

L'*accès aux données* est un type d'autorisation octroyé à l'ensemble de CA Enterprise Log Manager par le biais de la stratégie d'accès aux données par défaut, pour la classe de ressource CALM. Tous les utilisateurs ont accès à toutes les données, hormis celles dont l'accès est restreint par des filtres.

Accès ODBC et JDBC

L'accès ODBC et JDBC aux magasins de journaux d'événements CA Enterprise Log Manager prend en charge l'utilisation des données d'événements par un grand nombre de produits tiers, notamment la génération de rapports d'événements personnalisés à l'aide d'outils de génération de rapports tiers, la corrélation d'événements à l'aide de moteurs de corrélation et l'évaluation d'événements à l'aide de produits de détection d'intrusion et de programmes malveillants. Les systèmes Windows utilisent ODBC ; les systèmes UNIX ou Linux utilisent JDBC.

adaptateurs CA

Les *adaptateurs CA* constituent un groupe d'écouteurs qui reçoit des événements provenant de composants CA Audit tels que les clients CA Audit, les iRecorders et les SAPI Recorders, ainsi que les sources qui transmettent des événements de manière native via iTechnology.

agent

Un *agent* est un service générique, configuré avec des connecteurs chargés de collecter les événements bruts à partir d'une source d'événement unique, puis de les envoyer à CA Enterprise Log Manager pour traitement. Chaque CA Enterprise Log Manager dispose d'un agent intégré. De plus,vous pouvez installer un agent sur un point de collecte distant et collecter des événements sur des hôtes où l'installation d'agents est impossible. Vous pouvez également installer un agent sur l'hôte où s'exécutent les sources d'événement et bénéficier des possibilités d'application de règles de suppression et de chiffrement des transmissions vers CA Enterprise Log Manager.

agent par défaut

L'*agent par défaut* est l'agent intégré installé avec le serveur CA Enterprise Log Manager. Vous pouvez le configurer pour collecter directement des événements Syslog ainsi que des événements provenant de différentes sources non Syslog, par exemple CA Access Control r12 SP1, le service de certificats Microsoft Active Directory et les bases de données Oracle9i.

ajustement d'événement

L'*ajustement d'événement* est le processus par lequel une chaîne d'événement brut collecté est analysée en champs d'événement et mappée vers des champs CEG. Les utilisateurs peuvent exécuter des requêtes afin d'afficher les données d'événement ajusté ainsi obtenues. L'ajustement d'événement est l'étape qui suit la collecte des événements et qui précède leur stockage.

alerte d'action

Une *alerte d'action* est un job de requête planifié qui peut être utilisé pour détecter les violations de stratégie, les tendances d'utilisation, les schémas de connexion et d'autres actions d'événement nécessitant une attention à court terme. Par défaut, lorsque les requêtes d'une alerte renvoient des résultats, ces derniers sont affichés sur la page Alertes CA Enterprise Log Manager et ajoutés à un flux RSS. Lorsque vous planifiez une alerte, vous pouvez indiquer des destinations supplémentaires, y compris une adresse électronique, un processus de sortie d'événement/d'alerte CA IT PAM et des interruptions SNMP.

analyse

Le terme *analyse* (parfois analyse de message ou décomposition) désigne le processus d'extraction de données d'unités brutes et de conversion en paires de valeurs clés. L'analyse s'effectue sur la base d'un fichier XMP. Cette étape, qui précède le mappage de données, fait partie du processus d'intégration qui convertit les événements bruts collectés auprès d'une source d'événement en événements ajustés que vous pouvez consulter.

analyse (décomposition) d'un journal

L'*analyse (décomposition) d'un journal* est le processus qui permet d'extraire les données d'un journal, pour que les valeurs ainsi analysées (décomposées) puissent être utilisées lors des étapes suivantes du processus de gestion du journal.

analyse de fichiers XMP

L'*analyse de fichiers XMP* est le processus réalisé par l'utilitaire d'analyse de message pour rechercher tous les événements contenant chaque chaîne pré-associée, pour chaque événement associé, en décomposant l'événement en jetons à l'aide du premier filtre trouvé, qui utilise la même chaîne pré-associée.

analyse de mappage

L'*analyse de mappage* est une étape de l'Assistant de fichier de mappage, qui vous permet de tester et de modifier un fichier de mappage de données. Des exemples d'événement sont testés par rapport au fichier de mappage de données et les résultats sont validés avec la CEG.

analyse de message

L'*analyse de message* est le processus consistant à appliquer des règles à l'analyse d'un journal d'événements bruts, afin d'obtenir des informations pertinentes, telles que l'horodatage, l'adresse IP et le nom d'utilisateur. Les règles d'analyse utilisent la correspondance de caractères pour localiser un texte d'événement spécifique et le relier aux valeurs sélectionnées.

analyse des journaux

L'*analyse des journaux* est l'étude des entrées de journal, qui permet d'identifier les événements pertinents. Si les journaux ne sont pas analysés opportunément, leur valeur est considérablement réduite.

AppObjects

Les *AppObjects* (Application Objects), ou objets d'application, sont des ressources spécifiques à un produit ; ils sont stockés dans CA EEM sous l'instance d'application d'un produit donné. Pour l'instance d'application CAELM, ces ressources incluent le contenu des rapports et requêtes, les jobs planifiés pour les rapports et alertes, les configurations et le contenu des agents, les configurations de service, d'adaptateur et d'intégration, les fichiers de mappage de données et d'analyse de message, ainsi que les règles de suppression et de récapitulation.

archivage automatique

L'*archivage automatique* est un processus configurable qui permet d'automatiser le transfert des bases de données d'archivage entre deux serveurs. Lors de la première phase de l'archivage automatique, le serveur de collecte envoie les bases de données nouvellement archivées au serveur de rapports, à la fréquence que vous avez prédéfinie. Lors de la seconde phase, le serveur de rapports envoie les anciennes bases de données au serveur de stockage distant, pour un stockage à long terme, ce qui évite d'avoir à effectuer la sauvegarde et le transfert manuellement. Pour effectuer un archivage automatique, vous devez configurer une authentification sans mot de passe entre le serveur source et le serveur de destination.

archivage de journaux

L'*archivage de journaux* est le processus se déroulant lorsque la base de données chaude atteint sa taille maximale, auquel cas une compression au niveau des lignes est effectuée et la base passe de "l'état chaud" à "l'état tiède". Les administrateurs peuvent sauvegarder manuellement les bases de données tièdes, avant que le délai de suppression automatique ne soit écoulé, puis exécuter l'utilitaire LMArchive pour enregistrer le nom des sauvegardes. Ces informations sont alors disponibles à la consultation, via la requête d'archivage.

assistant de fichier d'analyse

L'*Assistant de fichier d'analyse* est une fonction CA Enterprise Log Manager que les administrateurs utilisent pour créer, modifier et analyser les fichiers d'analyse de message extensibles (XMP), stockés sur le serveur de gestion CA Enterprise Log Manager. Pour personnaliser l'analyse des données d'événements entrants, vous devez modifier les chaînes et filtres pré-associés. Les nouveaux fichiers, comme les fichiers modifiés, s'affichent dans l'Explorateur de collecte de journaux, la Bibliothèque d'ajustement d'événement, les fichiers d'analyse et le dossier Utilisateur.

balise

Une *balise* est un terme ou une expression clé, qui sert à identifier les requêtes ou rapports appartenant au même regroupement pertinent. Les balises permettent d'effectuer des recherches basées sur les regroupements pertinents. Le terme balise désigne également le nom de ressource utilisé dans une stratégie octroyant à l'utilisateur le droit de créer une balise.

bases de données archivées

Les *bases de données archivées* sur un serveur CA Enterprise Log Manager donné incluent : toutes les bases de données tièdes disponibles pour requête, mais nécessitant une sauvegarde manuelle avant expiration ; toutes les bases de données froides ; toutes les bases de données enregistrées comme restaurées à partir d'une sauvegarde.

bibliothèque d'ajustement d'événement

La *bibliothèque d'ajustement d'événement* est l'espace de stockage qui contient les intégrations, les fichiers de mappage et d'analyse, ainsi que les règles de suppression et de récapitulation, prédéfinis et définis par l'utilisateur.

bibliothèque d'analyse de message

La *bibliothèque d'analyse de message* est une bibliothèque qui accepte les événements provenant des files d'attente d'écouteur et qui utilise des expressions régulières pour marquer les chaînes en paires nom/valeur.

bibliothèque de la requête

La *bibliothèque de la requête* est la bibliothèque dans laquelle sont stockées toutes les requêtes, les balises de requête et les filtres d'invite, prédéfinis et définis par l'utilisateur.

bibliothèque de rapports

La *bibliothèque de rapports* est la bibliothèque dans laquelle sont stockés tous les rapports, les balises de rapports, les rapports générés et les jobs de rapports planifiés, prédéfinis et définis par l'utilisateur.

CA Enterprise Log Manager

CA Enterprise Log Manager est une solution qui vous permet de collecter des journaux à partir de sources d'événement très dispersées et de différents types, de contrôler la conformité avec les requêtes et les rapports, et de conserver des enregistrements des bases de données de journaux compressés stockées à long terme sur un système externe.

CA IT PAM

CA IT PAM est l'acronyme de CA IT Process Automation Manager. Le rôle de ce produit CA est d'automatiser les processus que vous définissez. CA Enterprise Log Manager utilise deux processus : la création d'un processus de sortie de l'événement/de l'alerte pour un produit local, par exemple CA Service Desk, et la génération dynamique de listes qui peuvent être importées sous la forme de valeurs à clés. L'intégration requiert CA IT PAM r2.1.

CA Spectrum

CA Spectrum est un produit de gestion des défaillances réseau qui peut être intégré à CA Enterprise Log Manager pour être utilisé comme destination des alertes envoyées sous la forme d'interruptions SNMP.

CAELM

CAELM est le nom de l'instance d'application que CA EEM utilise pour CA Enterprise Log Manager. Pour accéder à la fonctionnalité CA Enterprise Log Manager dans CA Embedded Entitlements Manager, saisissez l'URL https://<adresse_ip>:5250/spin/eiam/eiam.csp, sélectionnez CAELM comme nom d'application, puis saisissez le mot de passe de l'utilisateur EiamAdmin.

caelmadmin

Le nom d'utilisateur et le mot de passe *caelmadmin* sont les informations d'identification nécessaires pour accéder au système d'exploitation du dispositif logiciel. L'ID d'utilisateur caelmadmin est créé lors de l'installation de ce système d'exploitation. Durant l'installation du composant logiciel, l'installateur doit spécifier le mot de passe du compte de superutilisateur CA EEM, EiamAdmin. Le même mot de passe est affecté au compte caelmadmin. Nous recommandons que l'administrateur du serveur se connecte via ssh en tant qu'utilisateur caelmadmin et modifie ce mot de passe par défaut. Bien que l'administrateur ne puisse pas se connecter via ssh en tant que root, il peut basculer sur le compte root (su root) si nécessaire.

caelmservice

caelmservice est un compte de service qui permet d'exécuter iGateway et les services CA EEM locaux en tant qu'utilisateur non root. Le compte caelmservice est utilisé pour installer les mises à jour du système d'exploitation téléchargées avec les mises à jour d'abonnement.

calendrier

Un *calendrier* est un moyen de limiter la durée d'application d'une stratégie d'accès. Une stratégie permet aux identités spécifiées d'effectuer les actions indiquées sur la ressource spécifiée durant le laps de temps déterminé.

CALM

CALM est une classe de ressource prédéfinie qui inclue les ressources CA Enterprise Log Manager suivantes : Alerte, ArchiveQuery, calmTag, Données, EventGrouping, Intégration et Rapport. Les actions autorisées pour cette ressource sont : Annotation (Rapports), Création (Alerte, calmTag, EventGrouping, Intégration et Rapport), Dataaccess (Données), Exécution (ArchiveQuery) et Planification (Alerte, Rapport).

calmTag

calmTag est un attribut nommé de l'AppObject utilisé lors de la création d'une stratégie de portée afin de limiter l'accès aux requêtes et rapports appartenant à certaines balises. Tous les rapports et requêtes sont des objets d'application (AppObjects) et ont calmTag comme attribut (à ne pas confondre avec la balise de ressource).

catalogue

Le *catalogue* est la base de données stockée sur chaque CA Enterprise Log Manager, qui consigne l'état des bases de données archivées et joue le rôle d'index de haut niveau pour l'ensemble des bases de données. Les informations d'état (tiède, froid ou dégivré) sont conservées pour toutes les bases de données ayant jamais transité par ce CA Enterprise Log Manager, ainsi que toutes celles ayant été restaurées sur ce CA Enterprise Log Manager en tant que base de données dégivrée. La fonction d'indexation s'étend à toutes les bases de données chaudes et tièdes contenues dans le magasin de journaux d'événements de ce CA Enterprise Log Manager.

catalogue d'archive

Voir catalogue.

catégories d'événement

Les *catégories d'événement* sont les balises utilisées par CA Enterprise Log Manager pour classer les événements selon leur fonction, avant de les insérer dans le magasin d'événements.

Certificats

Les *certificats* prédéfinis utilisés par CA Enterprise Log Manager sont CAELMCert.p12 et CAELM_AgentCert.p12. Tous les services CA Enterprise Log Manager utilisent CALEMCert.p12 pour communiquer avec le serveur de gestion. Tous les agents utilisent CAELM_AgentCert.p12 pour communiquer avec leur serveur de collecte.

Champs CEG

Les champs CEG sont des étiquettes utilisées pour normaliser la présentation des champs d'événements bruts provenant de sources d'événement hétérogènes. Lors de l'ajustement d'événement, CA Enterprise Log Manager analyse les messages d'événements bruts dans une série de paires nom-valeur, puis mappe les noms des événements bruts avec les champs CEG standard. L'ajustement crée des paires nom-valeur composées des champs CEG et des valeurs issues de l'événement brut. En d'autres termes, au cours de l'ajustement des événements bruts, les différentes étiquettes utilisées dans les événements bruts correspondant au même objet de données ou élément de réseau sont converties au même nom de champ CEG. Les champs CEG sont mappés aux OID de la MIB utilisée pour les interruptions SNMP.

client d'abonnement

Un *client d'abonnement* est un serveur CA Enterprise Log Manager qui récupère les mises à jour de contenu auprès d'un autre serveur CA Enterprise Log Manager, appelé serveur proxy d'abonnement. Les clients d'abonnement interrogent le serveur proxy d'abonnement configuré de manière régulière et planifiée, et ils récupèrent les nouvelles mises à jour disponibles, le cas échéant. Après récupération des mises à jour, le client installe les composants téléchargés.

collecte d'événements

La *collecte d'événements* est un processus permettant de lire la chaîne d'événement brut à partir d'une source d'événement et de l'envoyer au CA Enterprise Log Manager configuré. La collecte est suivie d'un ajustement d'événement.

collecte directe de journaux

La *collecte directe de journaux* est la technique de collecte de journaux sans agent intermédiaire entre la source d'événement et le logiciel CA Enterprise Log Manager.

collecteur SAPI

Le *collecteur SAPI* est un adaptateur CA qui reçoit des événements provenant de clients CA Audit. Les envois des clients CA Audit reposent sur l'action Collecteur, qui propose le basculement intégré. Les administrateurs configurent le collecteur SAPI CA Audit avec, par exemple, les fichiers de mappage de données et les chiffres sélectionnés.

composants de visualisation

Les *composants de visualisation* sont des options disponibles pour l'affichage des données de rapport, par exemple une table, un graphique (en courbes, à barres, à colonnes, à secteurs) ou une visionneuse d'événements.

compte

Un *compte* est un utilisateur global qui est également un utilisateur d'applications CALM. Une même personne peut posséder plusieurs comptes, chacun disposant d'un rôle personnalisé différent.

configuration enregistrée

Une *configuration enregistrée* est une configuration stockée avec les valeurs d'attributs d'accès aux données provenant d'une intégration pouvant être utilisée comme modèle lors de la création d'une nouvelle intégration.

configuration globale

La *configuration globale* est un ensemble de paramètres qui s'appliquent à tous les serveurs CA Enterprise Log Manager utilisant le même serveur de gestion.

connecteur

Un *connecteur* est une intégration ciblant une source d'événement spécifique, configurée sur un agent donné. Un agent peut charger en mémoire plusieurs connecteurs, similaires ou non. Le connecteur permet de collecter les événements bruts à partir d'une source d'événement et d'effectuer une transmission régulée (sur règle) des événements convertis vers un magasin de journaux d'événements, où ils seront insérés dans la base de données chaude. Les intégrations prêtes à l'emploi permettent une collecte optimisée à partir d'une large gamme de sources d'événement, notamment des systèmes d'exploitation, des bases de données, des serveurs Web, des pare-feu et de nombreux types d'applications de sécurité. Vous pouvez définir entièrement un connecteur pour une source d'événement interne ou utiliser une intégration comme modèle.

Contenu d'une interruption SNMP

Une *interruption SNMP* se compose de paires nom-valeur, chaque nom étant un OID (identificateur d'objet) et chaque valeur une valeur renvoyée par l'alerte planifiée. Les résultats de requête renvoyés par une alerte d'action contiennent des champs CEG ainsi que leurs valeurs. L'interruption SNMP est renseignée en substituant un OID à chaque champ CEG utilisé pour le nom de la paire nom-valeur. Le mappage de chaque champ avec un OID est stocké dans la MIB. L'interruption SNMP inclut uniquement les paires nom-valeur des champs que vous avez sélectionnés lorsque de la configuration de l'alerte.

cumul d'événements

Le *cumul d'événements* est le processus par lequel des entrées de journal similaires sont regroupées en une entrée unique, contenant un compteur d'occurrences d'événement. Les règles de récapitulation définissent le regroupement des événements.

dégel

Le *dégel* est le processus qui consiste à faire passer une base de données de l'état froid à l'état dégivré. Cette opération est réalisée par CA Enterprise Log Manager lorsque l'utilitaire LMArchive l'avertit qu'une base de données froide connue a été restaurée. Si la base de données froide n'est pas restaurée sur son CA Enterprise Log Manager original, l'utilitaire LMArchive n'est pas utilisé et aucun dégel n'est requis ; la fonction de recatalogage ajoute la base de données restaurée en tant que base de données tiède.

Destinations d'une interruption SNMP

Lorsque vous planifiez une alerte d'action, vous avez la possibilité d'ajouter plusieurs *destinations pour l'interruption SNMP*. Chacune d'entre elles est définie par une adresse IP et un numéro de port. Généralement, la destination est un NOC ou un serveur de gestion tel que CA Spectrum ou CA NSM. Une interruption SNMP est envoyée aux destinations configurées lorsque les requêtes d'un job d'alerte planifié renvoient des résultats.

détecteur de journaux

Un *détecteur de journaux* est un composant d'intégration conçu pour lire un type de journal spécifique, comme une base de données, Syslog, un fichier ou SNMP. Les détecteurs de journaux peuvent être réutilisés. Généralement, les utilisateurs ne créent pas de détecteur de journaux personnalisé.

dispositif logiciel

Le *dispositif logiciel* comprend un composant système d'exploitation et le composant logiciel CA Enterprise Log Manager.

dossier

Un *dossier* est un emplacement de répertoire que le serveur de gestion CA Enterprise Log Manager utilise pour stocker les types d'objet CA Enterprise Log Manager. Vous référencez des dossiers dans des stratégies de portée afin de permettre ou d'interdire à certains utilisateurs d'accéder au type d'objet spécifié.

éléments d'intégration

Les *éléments d'intégration* incluent un détecteur, une aide à la configuration, un fichier d'accès aux données, un ou plusieurs fichiers d'analyse de message (XMP) et un ou plusieurs fichiers de mappage de données.

enregistrement de journal

Un *enregistrement de journal* est un enregistrement d'audit individuel.

enregistrements d'audit

Les *enregistrements d'audit* contiennent les événements de sécurité de type tentatives d'authentification, accès aux fichiers et modifications apportées aux stratégies de sécurité, comptes d'utilisateur ou droits d'utilisateur. Les utilisateurs Administrator spécifient les types d'événement à auditer et ce qui doit être journalisé.

entrée de journal

Une *entrée de journal* est, dans un journal, l'emplacement contenant des informations sur un événement spécifique qui s'est produit sur un système ou un réseau donné.

état chaud d'une base de données

L'*état chaud* correspond à une base de données du magasin de journaux d'événements, où sont insérés de nouveaux événements. Lorsqu'une base de données chaude atteint sa taille maximale prédéfinie sur le serveur de collecte, elle est compressée, cataloguée et déplacée sur un système de stockage non compressé sur le serveur de rapports. De plus, tous les serveurs stockent les nouveaux événements d'autosurveillance dans une base de données chaude.

état dégivré d'une base de données

L'*état dégivré* est l'état qualifiant une base de données qui a été restaurée dans le répertoire d'archivage après l'exécution de l'utilitaire LMArchive par l'administrateur pour indiquer à CA Enterprise Log Manager que la base de données a été restaurée. Les bases de données dégivrées sont conservées pendant le nombre d'heures configuré pour la stratégie d'exportation. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

état froid d'une base de données

L'*état froid* s'applique à une base de données tiède lorsqu'un administrateur exécute l'utilitaire LMArchive pour avertir CA Enterprise Log Manager que la base de données a été sauvegardée. Les administrateurs doivent sauvegarder les bases de données tièdes et exécuter cet utilitaire avant que ces bases de données ne soient supprimées. En effet, une base de données tiède est automatiquement supprimée lorsque son ancienneté dépasse la valeur Nbre max. de jours d'archivage définie ou lorsque le seuil Espace disque d'archivage est atteint, dès que l'une de ces deux conditions est remplie. Vous pouvez interroger la base de données d'archivage pour identifier les bases de données dont l'état est tiède ou froid.

état tiède d'une base de données

L'*état tiède* correspond à une base de données chaude de journaux d'événements, qui est déplacée lorsque sa taille atteint la limite maximale spécifiée (Nombre maximum de lignes) ou lorsqu'un recatalogage est effectué après restauration d'une base de données froide dans un nouveau magasin de journaux d'événements. Les bases de données tièdes sont conservées dans le magasin de journaux d'événements jusqu'à ce que leur ancienneté (en jours) dépasse la valeur configurée pour le paramètre Nbre max. de jours d'archivage. Vous pouvez effectuer des requêtes sur des journaux d'événements dans les bases de données chaudes, tièdes et dégivrées.

états de base de données

Les *états d'une base de données* incluent "chaude" pour une base de données de nouveaux événements, "tiède" pour une base de données d'événements compressés, "froide" pour une base de données sauvegardée et "dégivrée" pour une base de données restaurée dans le magasin de journaux d'événements où elle avait été sauvegardée. Vous pouvez lancer une requête sur les bases de données chaudes, tièdes et dégivrées. Toutes les requêtes d'archivage affichent les informations relatives aux bases de données froides.

événement ajusté

Un *événement ajusté* contient les données d'événements mappés ou analysés, dérivées d'événements bruts ou récapitulés. CA Enterprise Log Manager réalise le mappage et l'analyse pour permettre les recherches sur les données stockées.

événement brut

Un *événement brut* correspond aux informations déclenchées par un événement natif envoyé par un agent de surveillance au collecteur Log Manager. L'événement brut est souvent présenté sous la forme d'une chaîne Syslog ou d'une paire nom/valeur. Il est possible d'examiner un événement sous sa forme brute dans CA Enterprise Log Manager.

événement d'autosurveillance

Un *événement d'autosurveillance* est un événement journalisé par CA Enterprise Log Manager. Ce type d'événement est automatiquement généré sur la base d'actes effectués par l'utilisateur et de fonctions réalisées par différents modules, tels que les services et les écouteurs. Pour consulter le rapport précisant les détails des événements d'autosurveillance des opérations SIM, sélectionnez un serveur de rapports et ouvrez l'onglet Evénements d'autosurveillance.

événement distant

Un *événement distant* est un événement impliquant deux ordinateurs hôtes distincts, la source et la destination. Un événement distant est de type 2, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement enregistré

Un *événement enregistré* contient les données d'un événement brut ou ajusté, après son intégration dans la base de données. Les événements bruts sont toujours enregistrés, sauf s'ils sont supprimés ou récapitulés, comme des événements ajustés. Ces informations sont stockées et peuvent être interrogées.

événement local

Un *événement local* est un événement impliquant une entité unique, où la source et la destination de l'événement correspondent au même ordinateur hôte. Un événement local est de type 1, sur les quatre types d'événement utilisés dans la grammaire commune aux événements.

événement natif

Un *événement natif* constitue l'état ou l'action déclenchant un événement brut. Les événements natifs sont reçus et analysés/mappés, le cas échéant, puis transmis en tant qu'événements bruts ou ajustés. Un échec d'authentification est un événement natif.

événement observé

Un *événement observé* est un événement impliquant une source, une destination et un agent, où l'événement est observé et enregistré par un agent de collecte d'événements.

événement RSS

Un *événement RSS* est un événement généré par CA Enterprise Log Manager pour transmettre une alerte d'action à des produits et utilisateurs tiers. L'événement est un récapitulatif de chaque résultat d'alerte d'action et un lien vers le fichier de résultat. La durée d'un flux RSS donné peut être configurée.

événements

Dans CA Enterprise Log Manager, les *événements* sont des enregistrements de journal générés par chaque source d'événement spécifiée.

event_action

event_action est le champ de quatrième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il décrit les actions communes. Les types d'action d'événement (event_action) incluent par exemple : Lancement d'un processus, Arrêt d'un processus et Erreur d'application.

event_category

event_category est le champ de deuxième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur ideal_model spécifique. Les types de catégories d'événement (event_category) incluent : Sécurité opérationnelle, Gestion des identités, Gestion de la configuration, Accès aux ressources et Accès au système.

event_class

event_class est le champ de troisième niveau et spécifique à l'événement, utilisé par la grammaire commune aux événements (CEG) pour la normalisation des événements. Il permet une classification plus approfondie des événements, avec une valeur event_category spécifique.

explorateur d'agent

L'*Explorateur d'agent* est l'espace de stockage qui contient les paramètres de configuration d'un agent. Les agents peuvent être installés sur un point de collecte ou sur un terminal où il existe des sources d'événement.

fédération hiérarchique

Une *fédération hiérarchique* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation hiérarchique entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1, mais le serveur 1 n'est pas un enfant du serveur 2. La relation est donc unilatérale. Une fédération hiérarchique peut posséder de nombreux niveaux de relation parent-enfant et un seul serveur parent peut avoir de nombreux serveurs enfants. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et ses enfants.

fédération maillée

Une *fédération maillée* de serveurs CA Enterprise Log Manager est une topologie qui établit une relation de parité entre les serveurs. Dans sa forme la plus simple, le serveur 2 est un enfant du serveur 1 et le serveur 1 est un enfant du serveur 2. Une paire de serveurs maillée a une relation bilatérale. Une fédération maillée peut être définie pour qu'un grand nombre de serveurs soient les pairs les uns des autres. Une requête fédérée renvoie ses résultats depuis le serveur sélectionné et tous ses pairs.

fichier d'analyse de message (XMP, Message Parsing File)

Un *fichier d'analyse de message (XMP)* est un fichier XML associé à un type de source d'événement spécifique, qui applique des règles d'analyse. Les règles d'analyse décomposent les données pertinentes d'un événement brut collecté, afin d'obtenir des paires nom/valeur qui sont ensuite transmises au fichier de mappage de données à des fins de traitement. Ce type de fichier est utilisé dans toutes les intégrations, ainsi que dans les connecteurs, qui sont eux-mêmes basés sur des intégrations. Dans le cas d'adaptateurs CA, les fichiers XMP peuvent également être appliqués au serveur CA Enterprise Log Manager.

fichiers de mappage de données

Les *fichiers de mappage des données* sont des fichiers XML utilisant la grammaire commune aux événements (CEG) de CA pour transformer des événements d'un format source en un format conforme CEG pouvant être stocké à des fins de rapport et d'analyse dans le magasin de journaux d'événements. Un fichier de mappage de données doit être créé pour chaque nom de journal pour que les données d'événement puissent être stockées. L'utilisateur peut modifier une copie du fichier de mappage de données et l'appliquer à un connecteur spécifié.

filtrage d'événements

Le *filtrage d'événements* est le processus de tri des événements sur la base de filtres CEG.

filtre

Un *filtre* est un moyen permettant de limiter les requêtes sur le magasin de journaux d'événements.

filtre d'accès

Un *filtre d'accès* est un filtre que l'administrateur peut définir pour contrôler les données d'événement pouvant être consultées par les utilisateurs ou groupes ne détenant pas le rôle Administrator. Un filtre d'accès peut, par exemple, limiter les données que des identités spécifiées peuvent afficher dans un rapport. Les filtres d'accès sont automatiquement convertis en stratégies d'obligation.

filtre global

Un *filtre global* est un ensemble de critères que vous pouvez spécifier pour limiter les éléments présentés dans tous les rapports. Par exemple, un filtre global pour les 7 derniers jours renvoie les événements générés au cours des sept derniers jours écoulés.

filtre local

Un *filtre local* est un ensemble de critères que vous pouvez spécifier lors de la consultation d'un rapport, pour limiter les données affichées dans ce rapport en cours.

gestion des agents

La *gestion des agents* est le processus logiciel qui contrôle l'ensemble des agents associés à l'ensemble de CA Enterprise Log Manager fédérés. Ce processus authentifie les agents avec lesquels il communique.

gestion des droits

La *gestion des droits* est la méthode qui permet de contrôler ce que les utilisateurs sont autorisés à faire une fois authentifiés et connectés à l'interface CA Enterprise Log Manager. Ceci implique des stratégies d'accès associées à des rôles affectés aux utilisateurs. Ces rôles, ou groupes d'utilisateurs d'applications, et stratégies d'accès peuvent être prédéfinis ou définis par l'utilisateur. La gestion des droits est assurée par le magasin d'utilisateurs interne du système CA Enterprise Log Manager.

gestion des journaux de sécurité informatique

La *gestion des journaux de sécurité informatique* est définie par le National Institute of Standards and Technology (NIST) comme étant le "processus permettant de générer, de transmettre, de stocker, d'analyser et d'éliminer les données des journaux de sécurité des ordinateurs".

grammaire commune aux événements (CEG)

La *grammaire commune aux événements* est le cadre qui propose un format standard utilisé par CA Enterprise Log Manager pour convertir les événements à l'aide de fichiers d'analyse et de mappage, avant de les stocker dans le magasin de journaux d'événements. La CEG utilise des champs communs et normalisés pour définir les événements de sécurité provenant de plates-formes et de produits différents. Les événements ne pouvant faire l'objet d'une analyse ou d'un mappage sont stockés en tant qu'événements bruts.

groupe d'agents

Un *groupe d'agents* est une balise que les utilisateurs peuvent appliquer aux agents sélectionnés, qui permet d'appliquer simultanément une configuration à plusieurs agents et de récupérer les rapports basés sur les groupes. Un agent donné peut appartenir à un seul groupe à la fois. Les groupes d'agents sont basés sur des critères définis par l'utilisateur, comme la région géographique ou l'importance.

groupe d'applications

Un *groupe d'applications* est un groupe spécifique à un produit, pouvant être affecté à un utilisateur global. Les groupes d'applications (ou rôles) prédéfinis pour CA Enterprise Log Manager sont Administrator, Analyst et Auditor. Ces groupes d'applications sont disponibles uniquement pour les utilisateurs CA Enterprise Log Manager ; ils ne peuvent pas être affectés aux utilisateurs d'autres produits enregistrés sur le même serveur CA EEM. Des groupes d'applications définis par l'utilisateur doivent être ajoutés à la stratégie d'accès aux applications CALM par défaut, pour que les utilisateurs de ces groupes puissent accéder à CA Enterprise Log Manager.

groupe d'utilisateurs

Un *groupe d'utilisateurs* peut être un groupe d'applications, un groupe global ou un groupe dynamique. Les groupes d'applications CA Enterprise Log Manager prédéfinis sont les rôles Administrator, Analyst et Auditor. Les utilisateurs CA Enterprise Log Manager peuvent faire partie des groupes globaux par le biais d'appartenances distinctes de CA Enterprise Log Manager. Les groupes dynamiques sont définis par l'utilisateur et créés via une stratégie de groupe dynamique.

groupe d'utilisateurs dynamique

Un *groupe d'utilisateurs dynamique* est composé d'utilisateurs globaux qui partagent un ou plusieurs attributs communs. Un groupe d'utilisateurs dynamique est créé par le biais d'une stratégie de groupe d'utilisateurs dynamique particulière dans laquelle le nom de la ressource est le nom du groupe d'utilisateurs dynamique et l'appartenance repose sur un ensemble de filtres configurés sur les attributs d'utilisateur et de groupe.

groupe global

Un *groupe global* est un groupe partagé sur les instances d'application enregistrées auprès du même serveur de gestion CA Enterprise Log Manager. N'importe quel utilisateur peut être affecté à un ou plusieurs groupes globaux. Des stratégies d'accès peuvent être définies avec les groupes globaux en tant qu'identités, afin d'autoriser ou d'interdire à ces dernières d'effectuer certaines actions sur les ressources sélectionnées.

ideal_model

ideal_model correspond à la technologie exprimant l'événement. Il s'agit du premier champ de la grammaire commune aux événements (CEG) dans la hiérarchie des champs utilisés pour la normalisation et la classification des événements. Les types de modèles idéaux (ideal_model) incluent : Antivirus, DBMS, Pare-feu, Système d'exploitation et Serveur Web. Les produits de pare-feu Check Point, Cisco PIX et Netscreen/Juniper peuvent être normalisés en saisissant la valeur "Pare-feu" dans le champ ideal_model.

identité

Dans CA Enterprise Log Manager, une *identité* est un utilisateur ou un groupe autorisé à accéder à l'instance d'application CAELM et à ses ressources. Pour tout produit CA, une identité peut être un utilisateur global, un utilisateur d'applications, un groupe global, un groupe d'applications ou un groupe dynamique.

installateur

L'*installateur* est la personne qui se charge d'installer le dispositif logiciel et les agents. Lors de la procédure d'installation, les noms d'utilisateur caelmadmin et EiamAdmin sont créés et le mot de passe spécifié pour EiamAdmin est affecté à caelmadmin. Les informations d'identification de caelmadmin sont requises pour le premier accès au système d'exploitation ; celles de EiamAdmin sont nécessaires pour le premier accès au logiciel CA Enterprise Log Manager et pour l'installation des agents.

instance d'application

Une *instance d'application* est un espace commun dans le référentiel CA EEM, où sont stockés tous les utilisateurs, groupes, contenus, stratégies d'autorisation et configurations. En général, tous les serveurs CA Enterprise Log Manager d'une entreprise utilisent la même instance d'application (par défaut, CAELM). Vous pouvez installer des serveurs CA Enterprise Log Manager avec différentes instances d'application, mais seuls les serveurs partageant la même instance d'application peuvent être fédérés. Les serveurs configurés pour utiliser le même serveur CA EEM avec différentes instances d'application partagent uniquement le magasin d'utilisateurs, les stratégies de mots de passe et les groupes globaux. Les différents produits CA ont des instances d'application par défaut différentes.

intégration

L'*intégration* est une méthode permettant de traiter les événements non classés en événements ajustés, pour pouvoir les afficher dans les requêtes et les rapports. L'intégration est mise en oeuvre avec un ensemble d'éléments qui permettent à un connecteur et un agent donnés de collecter les événements à partir d'un ou de plusieurs types de source d'événement, puis de les envoyer à CA Enterprise Log Manager. Cet ensemble d'éléments inclut le détecteur de journaux ainsi que les fichiers XMP et de mappage de données, conçus pour être lus à partir d'un produit spécifique. Les intégrations permettant de traiter les événements Syslog et les événements WMI sont des exemples d'intégrations prédéfinies. Vous pouvez créer des intégrations personnalisées pour permettre le traitement d'événements non classés.

invite

Une *invite* est un type de requête spécial qui affiche des résultats en fonction de la valeur que vous saisissez et des champs CEG que vous sélectionnez. Les lignes sont uniquement renvoyées pour les événements dont la valeur saisie apparaît dans au moins un des champs CEG sélectionnés.

jeton d'analyse de message (ELM)

Un *jeton d'analyse de message* est un modèle réutilisable servant à la création de la syntaxe d'expression régulière utilisée lors de l'analyse de message CA Enterprise Log Manager. A chaque jeton sont associés un nom, un type et une chaîne d'expression régulière.

journal

Un *journal* est un enregistrement d'audit, ou message enregistré, concernant un événement ou un ensemble d'événements. Un journal peut afficher différents types : journal d'audit, journal de transaction, journal d'intrusion, journal de connexion, enregistrement des performances système, journal des activités utilisateur ou alerte.

liste de contrôle d'accès d'identité

Une *liste de contrôle d'accès d'identité* vous permet de spécifier différentes actions que chaque identité sélectionnée peut exécuter sur les ressources indiquées. Par exemple, avec une liste de contrôle d'accès d'identité, vous pouvez préciser qu'une identité donnée peut créer des rapports et qu'une autre peut planifier et annoter des rapports. La liste de contrôle d'accès d'identité diffère de la liste de contrôle d'accès classique dans le sens où elle est centrée sur l'identité, et non sur la ressource.

magasin de journaux d'événements

Le *magasin de journaux d'événements* est un composant du serveur CA Enterprise Log Manager, dans lequel les événements entrants sont stockés dans des bases de données. Les bases de données du magasin de journaux d'événements doivent être sauvegardées et déplacées manuellement vers un système de stockage distant de journaux, avant le délai de suppression configuré. Les bases de données archivées peuvent être restaurées dans un magasin de journaux d'événements.

magasin d'utilisateurs

Un *magasin d'utilisateurs* est le référentiel contenant les informations et stratégies de mots de passe d'utilisateurs globaux. Par défaut, le magasin d'utilisateurs CA Enterprise Log Manager est le référentiel local, mais il peut être configuré pour faire référence à CA SiteMinder ou à un répertoire LDAP pris en charge, comme Microsoft Active Directory, Sun One ou Novell eDirectory. Quelle que soit la configuration du magasin d'utilisateurs, le référentiel local sur le serveur de gestion contient des informations spécifiques aux applications concernant les utilisateurs, comme leur rôle et les stratégies d'accès associées.

mappage de données

Le *mappage de données* est un processus consistant à mapper les paires de valeurs clés vers la CEG. Le mappage de données s'effectue sur la base d'un fichier de mappage de données.

mappages de fonctions

Les *mappages de fonctions* constituent une partie facultative du fichier de mappage de données pour une intégration produit. Ils servent à renseigner un champ de la grammaire commune aux événements lorsque la valeur requise ne peut être extraite directement de la source d'événement. Tous les mappages de fonctions se composent d'un nom de champ CEG, d'une valeur de champ de classe ou prédéfinie, ainsi que de la fonction utilisée pour obtenir ou calculer la valeur.

MIB (base de données d'informations de gestion)

La *MIB (base de données d'informations de gestion)* pour CA Enterprise Log Manager, CA-ELM.MIB, doit être importée et compilée par chaque produit devant recevoir des alertes sous la forme d'interruptions SNMP depuis CA Enterprise Log Manager. La MIB indique l'origine de chaque identificateur d'objet numérique (OID) utilisé dans un message d'interruption SNMP accompagnée d'une description de l'objet de données ou de l'élément de réseau en question. Dans la MIB pour les interruptions SNMP envoyées par CA Enterprise Log Manager, la description de chaque objet de données est destinée au champ CEG associé. La MIB permet de s'assurer que toutes les paires nom-valeur transmises dans une interruption SNMP sont correctement interprétées au niveau de la destination.

mises à jour d'abonnement

Les *mises à jour d'abonnement* correspondent aux fichiers binaires et non binaires mis à disposition par le serveur d'abonnement CA. Les fichiers binaires sont des mises à jour du module produit, généralement installées sur les systèmes CA Enterprise Log Manager. Les fichiers non binaires, ou mises à jour de contenu, sont enregistrés sur le serveur de gestion.

mises à jour du contenu

Les *mises à jour de contenu* constituent la partie non binaire des mises à jour d'abonnement et elles sont enregistrées sur le serveur de gestion CA Enterprise Log Manager. Les mises à jour de contenu incluent les fichiers XMP, les fichiers de mappage de données, les mises à jour de configuration pour les modules CA Enterprise Log Manager et les mises à jour de clé publique.

module (à télécharger)

Un *module* est un groupement logique de mises à jour de composant, mis à disposition des utilisateurs en téléchargement, sur la base d'un abonnement. Un module peut contenir des mises à jour de fichier binaire, de contenu, ou les deux. Par exemple, tous les rapports sont réunis dans un même module ; toutes les mises à jour de fichier binaire de sponsor sont regroupées dans un autre module. CA définit le contenu de chaque module.

module d'abonnement

Le *module d'abonnement* est le service qui permet de télécharger automatiquement les mises à jour d'abonnement à partir du serveur d'abonnement CA et de les distribuer à tous les serveurs et agents CA Enterprise Log Manager. Les paramètres globaux s'appliquent aux serveurs CA Enterprise Log Manager locaux ; les paramètres locaux indiquent notamment si le serveur est un proxy hors ligne, un proxy en ligne ou un client d'abonnement.

module d'extension d'événements iTech

Le *module d'extension d'événements iTech* est un adaptateur CA qu'un administrateur peut configurer à l'aide de fichiers de mappage sélectionnés. Il reçoit des événements provenant d'iRecorders, de CA EEM, d'iTechnology ou de tout produit capable d'envoyer des événements via iTechnology.

NIST

Le *National Institute of Standards and Technology (NIST)* est l'agence technologique fédérale américaine qui propose des recommandations dans une publication intitulée "Special Publication 800-92 *Guide to Computer Security Log Management*" (en anglais), qui ont servi de base pour CA Enterprise Log Manager.

nom d'utilisateur EiamAdmin

EiamAdmin est le nom de superutilisateur par défaut affecté au programme d'installation des serveurs CA Enterprise Log Manager. Lors de l'installation du premier logiciel CA Enterprise Log Manager, le programme d'installation crée un mot de passe pour ce compte de superutilisateur, sauf si un serveur CA EEM distant existe déjà. Dans ce cas, le programme d'installation doit entrer le mot de passe existant. Une fois le dispositif logiciel installé, le programme d'installation ouvre un navigateur à partir d'une station de travail, entre l'URL de CA Enterprise Log Manager et se connecte en tant qu'utilisateur EiamAdmin avec le mot de passe associé. Ce premier utilisateur configure le magasin d'utilisateurs, crée les stratégies de mots de passe et crée le premier compte d'utilisateur doté du rôle Administrator. L'utilisateur EiamAdmin peut également effectuer n'importe quelle opération contrôlée par CA EEM.

OID (identificateur d'objet)

L'*OID (identificateur d'objet)* est l'identifiant numérique unique d'un objet de données apparié à une valeur dans un message d'interruption SNMP. Chaque OID utilisé dans une interruption SNMP envoyée par CA Enterprise Log Manager est mappé à un champ CEG dans la MIB. La syntaxe d'un OID mappé à un champ CEG est la suivante : 1.3.6.1.4.1.791.9845.x.x.x, où 791 est le numéro d'entreprise de CA et 9845 est l'identifiant produit de CA Enterprise Log Manager.

point de collecte

Un *point de collecte* est un serveur sur lequel un agent est installé ; sur le réseau, ce serveur est proche de tous les serveurs contenant les sources d'événements associées aux connecteurs de son agent.

pozFolder

pozFolder est un attribut d'AppObject, dont la valeur correspond à l'emplacement parent de l'AppObject. L'attribut et la valeur pozFolder sont utilisés dans les filtres de stratégies d'accès, qui restreignent l'accès aux ressources telles que les rapports, les requêtes et les configurations.

processus de sortie de l'événement/de l'alerte

Le *processus de sortie de l'événement/de l'alerte* est un processus CA IT PAM qui invoque un produit tiers pour répondre aux données d'alerte configurées dans CA Enterprise Log Manager. Vous pouvez sélectionner Processus CA IT PAM comme destination lorsque vous planifiez un job d'alerte. Lorsqu'une alerte déclenche l'exécution du processus CA IT PAM, CA Enterprise Log Manager envoie les données d'alerte CA IT PAM, lesquelles sont ensuite transférées par CA IT PAM avec leurs propres paramètres de traitement au produit tiers dans le cadre du processus de sortie de l'événement/de l'alerte.

profil

Un *profil* est un ensemble facultatif et configurable de filtres de données et de balises, qui peut être spécifique à un produit, à une technologie ou à une catégorie donnée. Le filtre de balise d'un produit, par exemple, limite les balises répertoriées à la balise du produit sélectionné. Les filtres de données d'un produit affichent uniquement les données pour le produit spécifié dans les rapports que vous générez, les alertes que vous planifiez et les résultats de requête que vous affichez. Une fois créé le profil de votre choix, vous pouvez le configurer de manière à ce qu'il soit appliqué dès que vous vous connectez au système. Si vous créez plusieurs profils, vous pouvez appliquer un profil différent à différentes activités, lors d'une même session. Des filtres prédéfinis sont livrés avec les mises à jour d'abonnement.

proxies d'abonnement (pour le client)

Les *proxies d'abonnement pour le client* définissent la liste des proxies d'abonnement que le client contacte de manière circulaire pour obtenir les mises à jour du système d'exploitation et du logiciel CA Enterprise Log Manager. Si un proxy est occupé, le suivant sur la liste est contacté. Si tous les proxies sont indisponibles et que le client est en ligne, le proxy d'abonnement par défaut est utilisé.

proxies d'abonnement (pour les mises à jour de contenu)

Les *proxies d'abonnement pour les mises à jour de contenu* sont les proxies d'abonnement choisis pour mettre à jour le serveur de gestion CA Enterprise Log Manager avec les mises à jour de contenu téléchargées sur le serveur d'abonnement CA. Il est recommandé de configurer plusieurs proxies, à des fins de redondance.

proxy d'abonnement (en ligne)

Un *proxy d'abonnement en ligne* est un serveur CA Enterprise Log Manager doté d'un accès à Internet et chargé de récupérer les mises à jour d'abonnement auprès du serveur d'abonnement CA, de manière régulière et planifiée. Un proxy d'abonnement en ligne donné peut être inclus dans la liste des proxies pour un ou plusieurs clients, qui contactent les proxies répertoriés de manière circulaire afin de demander les mises à jour de fichiers binaires. S'il est configuré pour le faire, un proxy en ligne donné peut envoyer les nouvelles mises à jour de contenu et de configuration au serveur de gestion, sauf si cela a déjà été fait par un autre proxy. Le répertoire des mises à jour d'abonnement d'un proxy en ligne sélectionné est utilisé comme source pour copier les mises à jour sur les proxies d'abonnement hors ligne.

proxy d'abonnement (hors ligne)

Un *proxy d'abonnement hors ligne* est un serveur CA Enterprise Log Manager qui obtient les mises à jour d'abonnement par une copie de répertoire manuelle (à l'aide de scp) depuis un proxy d'abonnement en ligne. Les proxies d'abonnement hors ligne peuvent être configurés pour télécharger les mises à jour de fichiers binaires sur les clients qui les demandent et pour envoyer la dernière version des mises à jour de contenu au serveur de gestion, si celui-ci ne l'a pas déjà reçue. Les proxies d'abonnement hors ligne n'ont pas besoin d'accès à Internet.

proxy d'abonnement (par défaut)

Le *proxy d'abonnement par défaut* est généralement le serveur CA Enterprise Log Manager installé en premier ; il peut également s'agir du serveur CA Enterprise Log Manager principal. Ce serveur sert également de proxy d'abonnement en ligne et doit, par conséquent, être doté d'un accès à Internet. Si aucun autre proxy d'abonnement en ligne n'est défini, ce serveur obtient les mises à jour d'abonnement auprès du serveur d'abonnement CA, puis télécharge les mises à jour de fichiers binaires sur tous les clients et envoie les mises à jour de contenu à CA EEM. Si d'autres proxies sont définis, le serveur obtient tout de même les mises à jour d'abonnement, mais il est contacté par les clients uniquement lorsque aucune liste de proxies d'abonnement n'est configurée ou lorsque la liste configurée est épuisée.

rapport

Un *rapport* est une représentation graphique ou tabulaire des données de journal d'événements qui est générée en exécutant des requêtes prédéfinies ou personnalisées à l'aide de filtres. Les données peuvent être issues de bases de données chaudes, tièdes et dégivrées dans le magasin de journaux d'événements du serveur sélectionné et, sur demande, de ses serveurs fédérés.

rapports EPHI

Les *rapports EPHI* (Electronic Protected Health Information) sont des rapports relatifs à la sécurité HIPAA (Health Insurance Portability and Accountability Act). Ces rapports peuvent vous aider à démontrer que toutes les informations médicales associées aux patients et identifiables individuellement, qui sont créées, stockées et transmises de manière électronique, sont protégées.

recatalogage

Le *recatalogage* est une révision forcée du catalogue. Un recatalogage est requis uniquement lors de la restauration de données dans un magasin de journaux d'événements situé sur un serveur différent de celui sur lequel les données ont été générées. Par exemple, si vous avez désigné CA Enterprise Log Manager comme point de restauration pour l'examen des données sauvegardées, vous devez imposer un recatalogage de la base de données après l'avoir restaurée depuis son point de restauration désigné. Un recatalogage est exécuté automatiquement au redémarrage d'iGateway, si nécessaire. Recataloguer un seul fichier de base de données peut prendre plusieurs heures.

règles de récapitulation

Les *règles de récapitulation* sont des règles combinant certains événements natifs, d'un même type, en un seul événement ajusté. Par exemple, une règle de récapitulation peut être configurée pour remplacer par un seul événement de récapitulation jusqu'à 1 000 événements dupliqués, dont les adresses IP et les ports source et de destination sont identiques. De telles règles simplifient l'analyse des événements et réduisent le trafic associé aux journaux.

règles de suppression

Les *règles de suppression* sont des règles que vous configurez pour éviter que certains événements ajustés n'apparaissent dans vos rapports. Vous pouvez créer des règles de suppression permanentes afin de supprimer des événements de routine sans rapport avec des problèmes de sécurité ; vous pouvez également créer des règles temporaires afin de supprimer la journalisation d'événements planifiés tels que la création de nombreux utilisateurs.

règles de transfert d'événement

Les règles de transfert d'événement stipulent que les événements sélectionnés sont transférés à des produits tiers, par exemple ceux qui mettent les événements en corrélation, après leur sauvegarde dans le magasin des journaux d'événements.

requête

Une *requête* est un ensemble de critères utilisés pour effectuer une recherche dans les magasins de journaux d'événements du serveur CA Enterprise Log Manager actif et, le cas échéant, de ses serveurs fédérés. Une requête cible les bases de données chaudes, tièdes ou dégivrées spécifiées dans la clause where de la requête. Par exemple, si la clause where limite la requête aux événements pour lesquels source_username="myname" sur une période donnée et que seules dix des 1 000 bases de données contiennent des enregistrements répondant à ces critères, sur la base des informations fournies dans la base de données de catalogue, la requête sera exécutée uniquement sur ces dix bases de données. Une requête peut renvoyer 5 000 lignes de données au maximum. Tout utilisateur doté d'un rôle prédéfini peut exécuter une requête. Seuls les analystes et les administrateurs peuvent planifier une requête pour diffuser une alerte d'action, créer un rapport en sélectionnant les requêtes à inclure, ou encore créer une requête personnalisée à l'aide de l'assistant de conception de requête. Voir également requête d'archivage.

requête d'action

Une *requête d'action* est une requête prenant en charge une alerte d'action. Elle est exécutée de manière planifiée et récurrente, pour tester les conditions définies par l'alerte d'action à laquelle elle est associée.

requête d'archivage

Une *requête d'archivage* est une requête du catalogue utilisée pour identifier les bases de données froides devant être restaurées et dégivrées à des fins de requête. Une requête d'archivage diffère d'une requête normale dans le sens où elle cible les bases de données froides, tandis que les requêtes normales ciblent uniquement les bases chaudes, tièdes et dégivrées. Les administrateurs peuvent émettre une requête d'archivage grâce à l'option Requête de catalogue d'archive du sous-onglet Collecte de journaux, dans l'onglet Administration.

ressource d'application

Le terme *ressource d'application* correspond à toutes les ressources spécifiques à CA Enterprise Log Manager, sur lesquelles les stratégies d'accès CALM autorisent ou interdisent à des identités données d'effectuer certaines actions spécifiques à l'application, par exemple créer, planifier et modifier. Rapport, alerte et intégration sont des exemples de ressource d'application. Voir également ressource globale.

ressource globale

Une *ressource globale*, pour le produit CA Enterprise Log Manager, est une ressource partagée avec les autres applications CA. Vous pouvez créer des stratégies de portée pour les ressources globales. Utilisateur, stratégie et calendrier sont des exemples de ressource globale. Voir également ressource d'application.

rôle Administrator

Le *rôle Administrator* accorde aux utilisateurs la possibilité d'effectuer toutes les actions valides existantes sur l'ensemble des ressources CA Enterprise Log Manager. Seuls les utilisateurs Administrator sont autorisés à configurer les services et la collecte de journaux, ou encore à gérer les utilisateurs, les stratégies d'accès et les filtres d'accès.

rôle Analyst

Le *rôle Analyst* accorde aux utilisateurs la possibilité de créer et de modifier des requêtes et rapports personnalisés, de modifier et d'annoter les rapports, de créer des balises, ou encore de planifier des rapports et alertes d'action. Les utilisateurs Analyst peuvent également réaliser toutes les tâches du rôle Auditor.

rôle Auditor

Le *rôle Auditor* accorde aux utilisateurs l'accès aux rapports et à leurs données. Les utilisateurs Auditor peuvent afficher les rapports, la liste des modèles de rapport, la liste des jobs de rapports planifiés et la liste des rapports générés. Les utilisateurs Auditor peuvent planifier et annoter des rapports. Ils n'ont pas accès aux flux RSS (Rich Site Summary), à moins qu'aucune authentification ne soit requise pour l'affichage des alertes d'action.

rôle d'utilisateur

Un *rôle d'utilisateur* peut être un groupe d'utilisateurs d'applications prédéfini ou un groupe d'applications défini par l'utilisateur. Des rôles d'utilisateur personnalisés sont nécessaires lorsque les groupes d'applications prédéfinis (Administrator, Analyst et Auditor) ne sont pas suffisamment affinés pour refléter les attributions de tâches. Les rôles d'utilisateur personnalisés nécessitent des stratégies d'accès personnalisées et une modification des stratégies prédéfinies pour inclure le nouveau rôle.

routeur SAPI

Le *routeur SAPI* est un adaptateur CA qui reçoit les événements provenant des intégrations, de type Mainframe, et les renvoie au routeur CA Audit.

SafeObject

SafeObject est une classe de ressource prédéfinie dans CA EEM. Il s'agit de la classe de ressource à laquelle appartient AppObjects, stockée dans la portée de l'application. Les utilisateurs définissant des stratégies et des filtres permettant d'accéder aux AppObjects se réfèrent à cette classe de ressource.

SAPI Recorder

SAPI Recorder était la technologie utilisée pour envoyer les données à CA Audit, avant l'apparition d'iTechnology. SAPI signifie Submit API (Application Programming Interface) ou API de soumission. Les enregistreurs CA Audit pour CA ACF2, CA Top Secret, RACF, Oracle, Sybase et DB2 sont des exemples de SAPI Recorders.

serveur d'abonnement CA

Le *serveur d'abonnement CA* est la source des mises à jour d'abonnement de CA.

serveur d'alerte

Le *serveur d'alerte* sert à stocker les alertes d'action et les jobs d'alerte d'action.

serveur de collecte

Le *serveur de collecte* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de collecte ajuste les journaux d'événement entrants, les intègre à la base de données chaude, compresse celle-ci et en effectue un archivage automatique ou bien la copie sur le serveur de rapports associé. Le serveur de collecte compresse la base de données chaude lorsqu'elle atteint la taille maximale prédéfinie et effectue un archivage automatique selon le planning indiqué.

serveur de gestion

Le *serveur de gestion* est un rôle attribué au premier serveur CA Enterprise Log Manager installé. Ce serveur CA Enterprise Log Manager contient le référentiel chargé de stocker le contenu de tous ses serveurs CA Enterprise Log Manager, notamment les stratégies. Ce serveur correspond généralement au proxy d'abonnement par défaut. Bien que cela ne soit pas recommandé dans la plupart des environnements de production, le serveur de gestion peut prendre en charge tous les rôles.

serveur de point de restauration

Le *serveur de point de restauration* est un rôle attribué à un serveur CA Enterprise Log Manager. Pour étudier des événements sauvegardés, vous pouvez transférer des bases de données depuis le serveur de stockage distant jusqu'au serveur de point de restauration à l'aide d'un utilitaire, puis ajouter ces bases au catalogue et exécuter les requêtes de votre choix. Transférer des bases de données froides vers un point de restauration dédié est une alternative intéressante à la restauration de ces bases sur le serveur de rapports original.

serveur de rapports

Le *serveur de rapports* est un rôle attribué à un serveur CA Enterprise Log Manager. Le serveur de rapports reçoit les bases de données tièdes archivées automatiquement en provenance d'un ou plusieurs serveurs de collecte. Il traite les requêtes, les rapports, ainsi que les alertes et les rapports planifiés.

serveur de rapports

Le *serveur de rapports* est le service qui stocke les informations de configuration, telles que le serveur de messagerie à utiliser lors de l'envoi des alertes par courriel, l'apparence des rapports enregistrés au format PDF, ainsi que la conservation des stratégies pour les rapports enregistrés sur le serveur de rapports et les alertes envoyées au flux RSS.

serveur de stockage distant

Le *serveur de stockage distant* est un rôle attribué à un serveur qui reçoit les bases de données archivées automatiquement en provenance d'un ou plusieurs serveurs de rapports. Le serveur de stockage distant conserve les bases de données froides pendant le nombre d'années requis. L'hôte distant utilisé pour le stockage ne dispose généralement pas d'un système CA Enterprise Log Manager ou autre. Pour l'archivage automatique, configurez une authentification non interactive.

serveur ODBC

Le *serveur ODBC* est le service configuré qui définit le port utilisé pour les communications entre le client ODBC ou JDBC et le serveur CA Enterprise Log Manager et détermine si le chiffrement SSL est activé ou non.

serveur proxy HTTP

Un *serveur proxy HTTP* est un serveur proxy qui joue le rôle de pare-feu et empêche le trafic Internet de pénétrer dans l'entreprise ou de la quitter, hormis via le proxy. Le trafic sortant peut spécifier un ID et un mot de passe pour contourner le serveur proxy. L'utilisation d'un serveur proxy HTTP local dans la gestion de l'abonnement est configurable.

serveurs de fédération

Les *serveurs de fédération* sont des serveurs CA Enterprise Log Manager connectés les uns aux autres sur un réseau, afin de répartir la collecte des données de journal, tout en cumulant les données collectées à des fins de génération de rapports. Les serveurs de fédération peuvent être connectés selon une topologie hiérarchique ou maillée. Les rapports de données fédérées incluent celles provenant du serveur cible, ainsi que de ses enfants ou pairs, le cas échéant.

services

Les *services* CA Enterprise Log Manager sont le magasin de journaux d'événements, le serveur de rapports et l'abonnement. Les administrateurs configurent ces services au niveau global, où tous les paramètres s'appliquent à l'ensemble de CA Enterprise Log Manager par défaut. La plupart des paramètres globaux de services peuvent être remplacés au niveau local, pour CA Enterprise Log Manager donné.

SNMP

SNMP est l'acronyme de Simple Network Management Protocol (protocole simple de gestion de réseau), une norme ouverte de transmission de messages d'alerte sous la forme d'interruptions SNMP depuis un agent vers un ou plusieurs systèmes de gestion.

source d'événement

Une *source d'événement* est l'hôte à partir duquel un connecteur collecte des événements bruts. Une source d'événement peut contenir plusieurs magasins de journaux, tous accessibles via un connecteur différent. En général, le déploiement d'un nouveau connecteur implique la configuration de la source d'événement de sorte que l'agent puisse y accéder et lire les événements bruts à partir de l'un de ses magasins de journaux. Les événements bruts du système d'exploitation, des bases de données différentes et une variété d'applications de sécurité sont stockés séparément sur la source d'événement.

stockage des journaux d'événements

Le *stockage des journaux d'événements* est le résultat du processus d'archivage, lorsque l'utilisateur sauvegarde une base de données tiède, avertit CA Enterprise Log Manager en exécutant l'utilitaire LMArchive et déplace la base de données sauvegardée depuis le magasin de journaux d'événements jusqu'à l'emplacement de stockage à long terme.

stratégie d'accès

Une *stratégie d'accès* est une règle qui accorde ou refuse à une identité (utilisateur ou groupe d'utilisateurs) des droits d'accès à une ressource d'application. CA Enterprise Log Manager détermine si les stratégies s'appliquent à l'utilisateur concerné en faisant correspondre les identités, les ressources, les classes de ressources et en évaluant les filtres.

stratégie d'accès aux applications CALM

La *stratégie d'accès aux applications CALM* est une stratégie de portée de type Liste de contrôle d'accès, qui détermine qui peut se connecter au serveur CA Enterprise Log Manager. Par défaut, la connexion est autorisée pour les rôles Administrator [Groupe], Analyst [Groupe] et Auditor [Groupe].

stratégie de délégation

Une *stratégie de délégation* est une stratégie d'accès qui permet à un utilisateur de déléguer son autorité à un autre utilisateur, groupe d'applications, groupe global ou groupe dynamique. Vous devez supprimer explicitement les stratégies de délégation créées par un utilisateur supprimé ou désactivé.

stratégie de portée

Une *stratégie de portée* est un type de stratégie d'accès qui octroie ou interdit l'accès aux ressources stockées sur le serveur de gestion, notamment les AppObjects, les utilisateurs, les groupes, les dossiers et les stratégies. Une stratégie de portée définit les identités pouvant accéder aux ressources spécifiées.

stratégie d'obligation

Une *stratégie d'obligation* est une stratégie générée automatiquement lorsque vous créez un filtre d'accès. Vous ne pouvez pas créer, modifier ou supprimer directement une stratégie d'obligation. Vous devez plutôt créer, modifier ou supprimer le filtre d'accès correspondant.

suppression

La *suppression* est le processus de tri des événements sur la base de filtres CEG. La suppression s'effectue sur la base de fichiers SUP.

traitement des valeurs dynamiques

Un *traitement des valeurs dynamiques* est un processus CA IT PAM que vous pouvez invoquer pour renseigner ou mettre à jour la liste de valeurs d'une clé donnée utilisée dans des rapports ou des alertes. Vous fournissez le chemin d'accès au traitement des valeurs dynamiques lors de la configuration de CA IT PAM dans la liste des services de serveurs de rapports de l'onglet Administration. Vous cliquez sur Importer la liste des valeurs dynamiques dans la section Valeur associée aux valeurs clés sur la même page de l'interface utilisateur. L'invocation du traitement des valeurs dynamiques est l'une des trois méthodes qui vous permettent d'ajouter des valeurs à vos clés.

URL de CA Embedded Entitlements Manager

L'*URL de CA Embedded Entitlements Manager* (CA EEM) est : https://<adresse_ip>:5250/spin/eiam. Pour ouvrir une session, sélectionnez CAELM comme application et saisissez le mot de passe associé au nom d'utilisateur EiamAdmin.

URL de CA Enterprise Log Manager

L'*URL de CA Enterprise Log Manager* est : https://<adresse_ip>:5250/spin/calm. Pour ouvrir une session, saisissez le nom d'utilisateur défini pour votre compte par l'administrateur, puis le mot de passe associé. Vous pouvez également saisir le nom de superutilisateur par défaut, EiamAdmin, puis entrer le mot de passe associé.

URL du flux RSS pour l'abonnement

L'*URL du flux RSS pour l'abonnement* est un lien préconfiguré, utilisé par les serveurs proxy d'abonnement en ligne lors de la récupération des mises à jour d'abonnement. Cette URL est destinée au serveur d'abonnement CA.

URL du flux RSS pour les alertes d'action

L'*URL du flux RSS pour les alertes d'action* est : https://{nomhôteelm}:5250/spin/calm/getActionQueryRssFeeds.csp. A partir de cette URL, vous pouvez afficher les alertes d'action soumises à la configuration définie en termes de quantité et d'ancienneté maximales.

utilisateur d'application

Un *utilisateur d'application* est un utilisateur global auquel ont été attribués des détails au niveau de l'application. Les détails d'utilisateur d'application CA Enterprise Log Manager incluent le groupe d'utilisateurs et les éventuelles restrictions d'accès. Si le magasin d'utilisateurs est le référentiel local, les détails de l'utilisateur d'application incluent également les informations d'identification de connexion et les stratégies de mots de passe.

utilisateur EEM

L'*utilisateur EEM*, configuré dans la section Archivage automatique du Magasin de journaux d'événements, spécifie l'utilisateur autorisé à exécuter une requête d'archivage, à recataloguer la base de données d'archivage, à exécuter l'utilitaire LMArchive et à exécuter le script shell restore-ca-elm pour restaurer les bases de données d'archivage à des fins d'examen. Cet utilisateur doit posséder le rôle prédéfini Administrator ou un rôle personnalisé associé à une stratégie personnalisée qui autorise l'action Modifier sur la ressource Base de données.

utilisateur global

Un *utilisateur global* se compose des informations de compte d'utilisateur, à l'exclusion des données propres aux applications. Les détails de l'utilisateur global et les appartenances au groupe global sont partagés par l'ensemble des applications CA intégrant le magasin d'utilisateurs par défaut. Les détails de l'utilisateur global peuvent être stockés dans le référentiel intégré ou dans un répertoire externe.

utilitaire LMArchive

LMArchive est l'utilitaire de ligne de commande qui suit la sauvegarde et la restauration des bases de données d'archive vers le magasin de journaux d'événements d'un serveur CA Enterprise Log Manager. Utilisez LMArchive pour effectuer une requête sur la liste des fichiers de bases de données tièdes, prêts à être archivés. Après avoir sauvegardé la base de données répertoriée et l'avoir transférée sur un stockage à long terme (froid), utilisez LMArchive pour créer un enregistrement sur CA Enterprise Log Manager, indiquant que cette base de données a été sauvegardée. Suite à la restauration d'une base de données froide sur son CA Enterprise Log Manager d'origine, utilisez LMArchive pour notifier CA Enterprise Log Manager, qui place alors les fichiers de bases de données dans un état dégivré, accessible aux requêtes.

utilitaire LMSEOSImport

LMSEOSImport est un utilitaire de ligne de commande utilisé pour importer SEOSDATA, ou des événements existants, dans CA Enterprise Log Manager dans le cadre de la migration depuis le générateur de rapports, la visionneuse ou le collecteur d'Audit. L'utilitaire est pris en charge uniquement par Microsoft Windows et Sun Solaris Sparc.

utilitaire scp

La copie sécurisée *scp* (programme de copie de fichiers à distance) est un utilitaire UNIX qui permet de transférer des fichiers entre les ordinateurs UNIX d'un réseau. Cet utilitaire est fourni lors de l'installation CA Enterprise Log Manager, pour que vous puissiez transférer les fichiers de mise à jour d'abonnement depuis le proxy d'abonnement en ligne jusqu'au proxy d'abonnement hors ligne.

valeurs clés

Les *valeurs clés* sont des valeurs définies par l'utilisateur et affectées à une liste définie par l'utilisateur (groupe clé). Lorsqu'une requête utilise un groupe clé, les résultats de la recherche incluent les correspondances avec toutes les valeurs clés du groupe. Il existe plusieurs groupes clés prédéfinis ; certains contiennent des valeurs clés prédéfinies, utilisées dans les requêtes et rapports prédéfinis.

Index

A

agent par défaut
    configuration du connecteur Syslog - 29
analyse de message
    définition - 53
archivage
    définition - 51

C

CA Embedded Entitlements Manager
    définition - 57
CA Enterprise Log Manager
    aide en ligne - 63
    composants - 12
    infobulles - 61
    installation - 12, 16
    rôles d'utilisateur - 58
clé d'authentification d'agent
    mise à jour - 36
collecte de journaux
    définition - 49
compte d'utilisateur des agents
    définie pour Windows - 35
connecteurs
    configuration - 41

E

environnement de test
    éléments installés - 12

F

fichiers binaires de l'agent
    télécharger pour les systèmes Windows - 37

G

gestion de l'abonnement
    définition - 59
    description de processus - 59
grammaire commune aux événements (CEG)
    définition - 53

I

infobulles
    utilisation - 61
installation de l'agent
    manuelle, pour Windows - 38
invites
    utilisation pour afficher des événements Syslog - 32
    utilisation pour afficher des journaux de sources d'événement Windows - 45

M

mappage de données
    définition - 53

R

rôles d'utilisateur
    définition - 58

S

stockage des journaux
    définition - 51
Syslog
    afficher des événements - 32